DEPARTMENT OF THE TREASURY
FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING

FINANCIAL FRAUD INSTITUTE

STUDENT TEXT

STATE COMPUTER CRIME STATUTES

DISCLAIMER

The Financial Fraud Institute has compiled this library of state statutes relating to computer crimes. Although every effort has been made to insure accuracy and timeliness, the user is encouraged to use this these citations strictly as a reference. For specific research, more thorough sources should be researched. These statutes should not be referenced without noting appropriate legislative histories, statutory notes, and judicial interpretations which will be found elsewhere. The statutes are, of course subject to change at any time.

Also be aware that these citations are generally restricted specifically to computer crime with only occasional references to related offenses. There is no particular reference herein to credit card fraud, telecommunications schemes, intellectual property offenses or other technically-oriented issues.

FFI acknowledges and appreciates the assistance of Abigail Abraham, Assistant District Attorney, Cook County, Illinois, in preparing this document.

Should the user encounter specific errors in this reference, or be aware of amendments, relevant additions, or repeal, it is requested that the Financial Fraud Institute be advised of such changes by writing:

Program Manager (CCTP)
Financial Fraud Institute
Bldg. 210, FLETC
Glynco, Georgia 31524
(912)267-2724

Table of Contents

CODE OF ALABAMA 1975

TITLE 13A. CRIMINAL CODE.
CHAPTER 8. OFFENSES INVOLVING THEFT.
ARTICLE 1. THEFT AND RELATED OFFENSES.

§13A-8-2 Theft of property -- Definition.

A person commits the crime of theft of property if he:

(1) Knowingly obtains or exerts unauthorized control over the property of another, with intent to deprive the owner of his property; or

(2) Knowingly obtains by deception control over the property of another, with intent to deprive the owner of his property.

(Acts 1977, No. 607, p. 812, §3201.)

§13A-8-10 Theft of services -- Definition.

(a) A person commits the crime of theft of services if:

(1) He intentionally obtains services known by him to be available only for compensation by deception, threat, false token or other means to avoid payment for the services; or

(2) Having control over the disposition of services of others to which he is not entitled, he knowingly diverts those services to his own benefit or to the benefit of another not entitled thereto.

(b) "Services" includes but is not necessarily limited to labor, professional services, transportation, telephone or other public services, accommodation in motels, hotels, restaurants or elsewhere, admission to exhibitions, computer services and the supplying of equipment for use.

(c) Where compensation for services is ordinarily paid immediately upon the rendering of them, as in the case of motels, hotels, restaurants and the like, absconding without payment or bona fide offer to pay is prima facie evidence under subsection (a) that the services were obtained by deception.

(d) If services are obtained under subdivision (a) (1) from a hotel, motel, inn, restaurant or cafe, no prosecution can be commenced after 120 days from the time of the offense.

(Acts 1977, No. 607, p. 812, §3210; Acts 1978, No. 770, p. 1110, §1; Acts 1979, No. 79-471, p. 862, §1.)

§13A-8-10.4 Theft of trademarks or trade secrets.

(a) For purposes of this section:

(1) Article. Any object, material, device, or substance or any copy thereof, including a writing, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint, or map.

(2) Copy. A facsimile, replica, photograph, or other reproduction of an article or a note, drawing, or sketch made of or from an article.

(3) Representing. Describing, depicting, containing, constituting, reflecting, or recording.

(4) Trade secret. The whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes.

(5) Trademark. Any word, name, symbol, or device adopted and used by any person or business entity to identify his goods or services, and to distinguish them from the goods or services of others.

(b) A person commits the crime of "theft of trade secrets or trademarks" if, without the owner's effective consent, he knowingly:

(1) Steals a trade secret;

(2) Makes a copy of an article representing a trade secret;

(3) Communicates or transmits a trade secret;

(4) Makes a copy or reproduction of a trademark for any commercial purpose; or

(5) Sells an article on which a trademark is reproduced knowing said trademark was used without the owner's consent.

(c) Theft of trade secrets or trademarks is a Class C felony.

CODE OF ALABAMA 1975

TITLE 13A. CRIMINAL CODE.
CHAPTER 8. OFFENSES INVOLVING THEFT.
ARTICLE 5. ALABAMA COMPUTER CRIME ACT.

§13A-8-100 Short title.

This article may be cited as the Alabama Computer Crime Act.

§13A-8-101 Definitions.

When used in this chapter, the following terms shall have the following meanings, respectively, unless a different meaning clearly appears from the context:

(1) Data. A representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and should be classified as intellectual property, and may be in any form, including computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

(2) Intellectual property. Data, including computer program.

(3) Computer program. An ordered set of data representing coded instructions or statements that, when executed by a computer, cause the computer to process data.

(4) Computer. An electronic magnetic, optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

(5) Computer software. A set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system or computer network.

(6) Computer system. A set of related, connected or unconnected, computer equipment, devices, or computer software.

(7) Computer network. A set of related, remotely connected devices and communication facilities, including more than one computer system, with capability to transmit data among them through communication facilities.

(8) Computer system services. The utilization of a computer, computer system, or computer network to assist an individual or entity with the performance of a particular lawful function which that individual or entity has been given the right, duty, and power, together with the responsibility, to perform.

(9) Property. Anything of value as defined by law, and includes financial instruments, information, including electronically produced data and computer software and computer

programs in either machine or human readable form, and any other tangible or intangible items of value.

(10) Financial instrument. Includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(11) Access. To instruct, communicate with, store data in, or retrieve data from a computer, computer system or computer network.

§13A-8-102 Acts constituting offenses against intellectual property; punishment.

(a) Whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, attempts or achieves access, communication, examination, or modification of data, computer programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(b) Whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, destroys data, computer programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(c) Whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, discloses, uses, or takes data, computer programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(d) (1) Except as otherwise provided in this subsection, an offense against intellectual property is a Class A misdemeanor, punishable as provided by law.

(2) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a Class C felony, punishable as provided by law.

(3) If the damage to such intellectual property is $2,500.00 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public or utility service, then the offender is guilty of a Class B felony, punishable as provided by law.

(4) Whoever willfully, knowingly, and without authorization alters or removes data causing physical injury to any person who is not involved in said act shall be guilty of a Class A felony, punishable as provided by law.

§13A-8-103 Acts constituting offense against computer equipment or supplies; punishment.

(a) (1) Whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, modifies equipment or supplies that are used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(2) a. Except as provided in this subsection, an offense against computer equipment or supplies as provided in subdivision (a)(1) is a Class A misdemeanor, punishable as provided by law.

b. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a Class C felony, punishable as provided by law.

(b) (1) Whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, destroys, uses, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network, or whoever willfully, knowingly, and without authorization or without reasonable grounds to believe that he has such authorization, destroys, injures, takes, or damages any computer, computer system, or computer network commits an offense against computer equipment and supplies.

(2) a. Except as provided in this subsection, an offense against computer equipment or supplies as provided in subdivision (b)(1) is a Class A misdemeanor, punishable as provided by law.

b. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $2,500.00 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public utility service, then the offender is guilty of a Class B felony, punishable as provided by law.

ALASKA STATUTES

Title 11. Criminal Law.
Chapter 46. Offenses Against Property.
Article 5. Business and Commercial Offenses.

Current with Ch. 255, approved 7-14-92

Sec. 11.46.740 Criminal use of computer.

(a) A person commits the offense of criminal use of a computer if, having no right to do so or any reasonable ground to believe the person has such a right,the person knowingly accesses or causes to be accessed a computer, computer system, computer program, computer network, or any part of a computer system or network, and as a result of that access

(1) obtains information concerning a person; or
(2) introduces false information into a computer, computer system, or computer network with the intent to damage or enhance the data record of a person.

(b) Criminal use of a computer is a class C felony.
(§ 3 ch 79 SLA 1984)

REFERENCES

Collateral references. -- Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 ALR4th 1046.

ARIZONA REVISED STATUTES ANNOTATED

TITLE 13. CRIMINAL CODE
CHAPTER 16. CRIMINAL DAMAGE TO PROPERTY

§13-1602. Criminal damage; classification

A. A person commits criminal damage by recklessly:

1. Defacing or damaging property of another person; or
2. Tampering with property of another person so as substantially to impair its function or value; or
3. Tampering with the property of a utility.
4. Parking any vehicle in such a manner as to deprive livestock of access to the only reasonably available water.

B. Criminal damage is punished as follows:

1. Criminal damage is a class 4 felony if the person recklessly damages property of another in an amount of ten thousand dollars or more, or if the person recklessly causes impairment of the functioning of any utility

. . .

SELECTED LEGISLATIVE HISTORY

Although definition of common criminal damage did not include language "without the express permission of the owner," absence of property owner's permission was a necessary and implicit element of the crime. State v. Moran (App.1989) 162 Ariz. 524, 784 P.2d 730.

Computer programmer did not criminally damage his employer's computer program by encoding it, where he had employer's permission to do so. State v. Moran (App.1989) 162 Ariz. 524, 784 P.2d 730.

Computer programmer's refusal to follow his employer's directive to decode a program he had prepared in an encoded state with his employer's permission was an omission, not an act, and thus not proscribed by this section defining criminal damage as "tampering." State v. Moran (App.1989) 162 Ariz. 524, 784 P.2d 730.

§ 13-2316. Computer fraud; classification

A. A person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such computer, system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

B. A person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in

such computer, computer system or computer network.

C. Computer fraud in the first degree is a class 3 felony. Computer fraud in the second degree is a class 6 felony.

SELECTED LEGISLATIVE HISTORY

In prosecution for first-degree computer fraud and other offenses, evidence that defendant, who had raped and murdered victim, used victim's bank card to access bank's automated teller machine system and to obtain funds therefrom was sufficient to sustain conviction of computer fraud. State v. Gillies (1983) 135 Ariz. 500, 662 P.2d 1007, appeal after remand 142 Ariz. 564, 691 P.2d 655, certiorari denied 105 S.Ct. 1775, 470 U.S. 1059, 84 L.Ed.2d 834.

This section's computer fraud provision does not authorize forfeiture of property used in commission of that crime. In re Commodore 128 Personal Computer With Accessories (App.1990) 166 Ariz. 567, 804 P.2d 100, review denied.

ARKANSAS CODE OF 1987 ANNOTATED

TITLE 5. CRIMINAL OFFENSES
SUBTITLE 4. OFFENSES AGAINST PROPERTY
CHAPTER 41. COMPUTER-RELATED CRIMES

5-41-101. Purpose.

It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer- related crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a statute be enacted which deals directly with computer-related crime.
History. Acts 1987, No. 908, s 1.

5-41-102. Definitions.

As used in this chapter, unless the context otherwise requires:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network;

(2) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses and includes all input, output, processing, storage, computer software, and communication facilities that are connected or related to that device in a system or a network;

(3) "Computer network" means the interconnection of communications lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers;

(4) "Computer program" means a set of instructions, statements, or related data that, in actual or modified form, is capable of causing a computer or a computer system to perform specified functions;

(5) "Computer software" means one (1) or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation;

(6) "Computer system" means a set of related, connected, or unconnected computers, other devices, and software;

(7) "Data" means any representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared and are intended to be processed or stored, are being processed or stored, or have been processed or stored in a computer, computer network, or computer system;

(8) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof;

(9) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computers and computer programs, or copies thereof, whether tangible or intangible, including both human and computer readable data, and data while in transit;

(10) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, a computer program, or data.

5-41-103. Computer fraud.

(a) Any person commits computer fraud who intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purpose of:

(1) Devising or executing any scheme or artifice to defraud or extort; or

(2) Obtaining money, property, or services with false or fraudulent intent, representations, or promises.

(b) Computer fraud is a Class D felony.

5-41-104. Computer trespass.

(a) Any person commits computer trespass who intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data.

(b) Computer trespass is a Class C misdemeanor if it is a first violation which does not cause any loss or damage.

(c) Computer trespass is a Class B misdemeanor if:

(1) It is a second or subsequent violation which does not cause any loss or damage; or

(2) It is a violation which causes loss or damage of less than five hundred dollars ($500).

(d) Computer trespass is a Class A misdemeanor if it is a violation which causes loss or damage of five hundred dollars ($500) or more, but less than two thousand five hundred dollars ($2,500).

(e) Computer trespass is a Class D felony if it is a violation which causes loss or damage

of two thousand five hundred dollars ($2,500) or more.

5-41-105. Venue of violations.

For the purpose of venue under this chapter, any violation of this chapter shall be considered to have been committed in any county:

(1) In which any act was performed in furtherance of any course of conduct which violated this chapter;

(2) In which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, data, or other material or objects which were used in furtherance of the violation;

(3) From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;

(4) In which any computer, computer system, or computer network is an object or an instrument of the violation is located at the time of the alleged violation.

5-41-106. Civil actions.

(a) Any person whose property or person is injured by reason of a violation of any provision of this chapter may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

(b) At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible reoccurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(c) No civil action under this section may be brought except within three (3) years from the date the alleged violation of this chapter is discovered or should have been discovered by the exercise of reasonable diligence.

5-41-107. Assistance of Attorney General.

If requested to do so by a prosecuting attorney, the Attorney General may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or any other offense involving the use of a computer.

ANNOTATED CALIFORNIA CODES

PENAL CODE
PART 2. OF CRIMINAL PROCEDURE
TITLE 8. OF JUDGMENT AND EXECUTION
CHAPTER 1. THE JUDGMENT

§1203.044. Economic Crime Act of 1992

(a) This section shall apply only to a defendant convicted of a felony for theft of an amount exceeding fifty thousand dollars ($50,000) in a single transaction or occurrence. This section shall not apply unless the fact that the crime involved the theft of an amount exceeding fifty thousand dollars ($50,000) in a single transaction or occurrence is charged in the accusatory pleading and either admitted by the defendant in open court or found to be true by the trier of fact. Aggregate losses from more than one criminal act shall not be considered in determining if this section applies.

(b) Notwithstanding any other law, probation shall not be granted to a defendant convicted of a crime to which subdivision (a) applies if the defendant was previously convicted of an offense for which an enhancement pursuant to Section 12022.6 was found true even if that enhancement was not imposed by the sentencing court. The prior conviction shall be alleged in the accusatory pleading and either admitted by the defendant in open court or found to be true by the trier of fact.

(c) In deciding whether to grant probation to a defendant convicted of a crime to which subdivision (a) applies, the court shall consider all relevant information, including the extent to which the defendant has attempted to pay restitution to the victim between the date upon which the defendant was convicted and the date of sentencing. A defendant claiming inability to pay restitution before the date of sentencing shall provide a statement of assets, income, and liabilities, as set forth in subdivision (j) to the court, the probation department, and the prosecution.

(d) In addition to the restrictions on probation imposed by subdivisions (b) and (c), probation shall not be granted to any person convicted of theft in an amount exceeding one hundred thousand dollars ($l00,000) in a single transaction or occurrence, except in unusual cases if the interests of justice would best be served if the person is granted probation. The fact that the theft was of an amount exceeding one hundred thousand dollars ($100,000) in a single transaction or occurrence, shall be alleged in the accusatory pleading and either admitted by the defendant in open court or found to be true by the trier of fact. This subdivision shall not authorize a grant of probation otherwise prohibited under subdivision (b) or (c). If probation is granted pursuant to this subdivision, the court shall specify on the record and shall enter on the minutes the circumstances indicating that the interests of justice would best be served by that disposition. Aggregate losses from more than one criminal act shall not be considered in determining whether this subdivision applies.

(e) Subject to subdivision (f), if a defendant is convicted of a crime to which subdivision (a) applies and the court grants probation, a court shall impose at least a 90-day sentence in a county jail as a condition of probation. If the defendant was convicted of a crime to which subdivision (d) applies, and the court grants probation, the court shall impose at least a 180-day sentence in a county jail as a condition of probation.

(f) The court shall designate a portion of any sentence imposed pursuant to subdivision (e) as a mandatory in-custody term. For the purpose of this section only, "mandatory in-custody term" means that the defendant shall serve that term, notwithstanding credits pursuant to Section 4019, in custody in the county jail. The defendant shall not be allowed release on any program during that term, including work furlough, work release, public service program, or electronic monitoring. The court shall designate the mandatory in-custody term as follows:

(1) If the defendant was convicted of a crime to which subdivision (a) applies the mandatory in-custody term shall be no less than 30 days. If the person serves a mandatory in-custody term of at least 30 days, the court may, in the interests of justice, and for reasons stated in the record, reduce the mandatory minimum 90-day sentence required by subdivision (e).

(2) If the defendant was convicted of a crime to which subdivision (d) applies, the mandatory in-custody term shall be no less than 60 days. If the person serves a mandatory in-custody term of at least 60 days, the court may, in the interests of justice, and for reasons stated in the record, reduce the mandatory minimum 180-day sentence required by subdivision (e).

(g) If a defendant is convicted of a crime to which subdivision (a) applies, and the court grants probation, the court shall require the defendant as a condition of probation to pay restitution to the victim and to pay a surcharge to the county in the amount of 20 percent of the restitution ordered by the court, as follows:

(1) The surcharge is not subject to any assessments otherwise imposed by Section 1464. The surcharge shall be paid into the county treasury and placed in the general fund to be used exclusively for the investigation and prosecution of white collar crime offenses and to pay the expenses incurred by the county in administering this section, including increased costs incurred as a result of offenders serving mandatory in-custody terms pursuant to this section.

(2) The court shall also enter an income deduction order as provided in Section 13967.2 of the Government Code to secure payment of the surcharge. That order may be enforced to secure payment of the surcharge as provided by those provisions.

(3) The county board of supervisors shall not charge the fee provided for by Section 1203.1 of this code or subdivision (d) of Section 13967 of the Government Code for the collection of restitution or any restitution fine.

(4) The defendant shall not be required to pay the costs of probation as otherwise required by subdivision (b) of Section 1203.1.

(h) Notwithstanding any other law, if a defendant is convicted of a crime to which subdivision (a) applies and the court grants probation, as a condition of probation, within 30 court days after being granted probation, and annually thereafter, the defendant shall provide the county financial officer with all of the following documents and records:

(1) True and correct copies of all income tax and personal property tax returns for the previous tax year, including W-2 forms filed on the defendant's behalf with any state tax agency. If the defendant is unable to supply a copy of a state tax return, the defendant shall provide a true and correct copy of all income tax returns for the previous tax year filed on his or her behalf with the federal government. The defendant is not required to provide any particular document if to do so would violate federal law or the law of the state in which the document was filed. However, this section shall supersede all other laws in this state concerning the right to privacy with respect to tax returns filed with this state. If, during the term of probation, the defendant intentionally fails to provide the county financial officer with any document that he or she knows is required to be provided under this subdivision, that failure shall constitute a violation of probation.

(2) A statement of income, assets, and liabilities as defined in subdivision (j).

(i) The submission by the defendant of any tax document pursuant to paragraph (1) of subdivision (h) that the defendant knows does not accurately state the defendant's income, or if required, the defendant's personal property, if the inaccuracy is material, constitutes a violation of probation.

(j) A statement of income, assets, and liabilities form, that is consistent with the disclosure requirements of this section, may be established by the financial officer of each county. That statement shall require the defendant to furnish relevant financial information identifying the defendant's income, assets, possessions, or liabilities, actual or contingent. The statement may include the following:

(1) All real property in which the defendant has any interest.

(2) Any item of personal property worth more than three thousand dollars ($3,000) in which the defendant has any interest, including, but not limited to, vehicles, airplanes, boats, computers, and consumer electronics. Any collection of jewelry, coins, silver, china, artwork, antiques, or other collectibles in which the defendant has any interest, if that collection is worth more than three thousand dollars ($3,000).

(3) All domestic and foreign assets in the defendant's name, or in the name of the defendant's spouse or minor children, of a value over three thousand dollars ($3,000) and in whatever form, including, but not limited to, bank accounts, securities, stock options, bonds, mutual funds, money market funds, certificates of deposits, annuities, commodities, precious metals, deferred compensation accounts, individual retirement accounts, and related or analogous accounts.

(4) All insurance policies in which the defendant or the defendant's spouse or minor children retain a cash value.

(5) All pension funds in which the defendant has a vested right.

(6) All insurance policies of which the defendant is a beneficiary.

(7) All contracts, agreements, judgments, awards, or prizes granting the defendant the right to receive money or real or personal property in the future, including alimony and child support.

(8) All trusts of which the defendant is a beneficiary.

(9) All unrevoked wills of a decedent if the defendant or defendant's spouse or minor child is a beneficiary.

(10) All lawsuits currently maintained by the defendant or by or against a corporation in which the defendant owns more than a 25 percent interest if the suit includes a prayer for damages.

(11) All corporations of which the defendant is an officer. If the defendant is an officer in a corporation sole, subchapter S corporation, or closely held corporation, and controls more equity of that corporation than any other individual, the county financial officer shall have authority to request other records of the corporation.

(12) All debts in excess of three thousand dollars ($3,000) owed by the defendant to any person or entity.

(13) Copies of all applications for loans made by the defendant during the last year.

(14) All encumbrances on any real and personal property in which the defendant has any interest.

(15) All sales, transfers, assignments, quitclaims, conveyances, or encumbrances of any interest in real or personal property of a value exceeding three thousand dollars ($3,000) made by the defendant during the period beginning one year before charges were filed to the present, including the identity of the recipient of same, and relationship, if any, to the defendant.

(k) The information contained in the statement of income, assets, and liabilities shall not be available to the public. Information received pursuant to this subdivision shall not be disclosed to any member of the public. Any disclosure in violation of this section shall be a contempt of court punishable by a fine not exceeding one thousand dollars ($1,000), and shall also create a civil cause of action for damages.

(l) After providing the statement of income, assets, and liabilities, the defendants shall provide the county financial officer with copies of any documents representing or reflecting the financial information set forth in subdivision (j) as requested by that officer.

(m) The defendant shall sign the statement of income, assets, and liabilities under penalty of

perjury. The provision of information known to be false, or the intentional failure to provide material information knowing that it was required to have been provided, shall constitute a violation of probation.

(n) The Franchise Tax Board and the Employment Development Department shall release copies of income tax returns filed by the defendant and other information concerning the defendant's current income and place of employment to the county financial officer upon request. That information shall be kept confidential and shall not be made available to any member of the public. Any unauthorized release shall be subject to subdivision (k). The county shall reimburse the reasonable administrative expenses incurred by those agencies in providing this information.

(o) During the term of probation, the defendant shall notify the county financial officer in writing within 30 days, after receipt from any source of any money or real or personal property that has a value of over five thousand dollars ($5,000), apart from the salary from the defendant's and the defendant's spouse's regular employment. The defendant shall report the source and value of the money or real or personal property received. This information shall not be made available to the public or the victim. Any unauthorized release shall be subject to subdivision (k).

(p) The term of probation in all cases shall be 10 years. However, after the defendant has served five years of probation, the defendant shall be released from all terms and conditions of probation except those terms and conditions included within this section. A court may not revoke or otherwise terminate probation within 10 years unless and until the defendant has satisfied both the restitution judgment and the surcharge, or the defendant is imprisoned for a violation of probation. Upon satisfying the restitution judgment, the defendant is entitled to a court order vacating that judgment and removing it from the public record. Amounts owing on the surcharge are forgiven upon completion of the term of probation.

(q) The county financial officer shall establish a suggested payment schedule each year to ensure that the defendant remits amounts to make restitution to the victim and pay the surcharge. The county financial officer shall evaluate the defendant's current earnings, earning capacity, assets (including assets that are in trust or in accounts where penalties may be incurred upon premature withdrawal of funds), and liabilities, and set payments to the county based upon the defendant's ability to pay. If the defendant objects to the suggested payment schedule, the court shall set the schedule. After the payment schedule is set, a defendant may request a change in the schedule upon a change of circumstances. The restitution schedule shall set a reasonable payment amount and shall not set payments in an amount that is likely to cause severe financial hardship to the defendant or his or her family.

(r) The willful failure to pay the amounts required by the payment schedule or to comply with the requirements of the county financial officer or the probation department pursuant to this section, if the defendant is able to pay or comply, is a violation of probation.

(s) In determining the defendant's ability to pay, the court shall consider whether the annual

payment required, including any money or property seized to satisfy the restitution judgment, exceeds 15 percent of the defendant's taxable income for the previous year as identified on the defendant's tax return for the defendant's state of residence or on the defendant's federal tax return. If the defendant has filed a joint return, the defendant's income for purposes of this section shall be presumed to be the total of all wages earned by the defendant, plus one-half of all other nonsalary income listed on the tax return and accompanying schedules, unless the defendant demonstrates otherwise. The court shall also consider the defendant's current income.

(t) The defendant shall personally appear at any hearing held pursuant to any provision of this section unless the defendant is incarcerated or otherwise excused by the court, in which case the defendant may appear through counsel.

(u) Notwithstanding subdivision (d) of Section 1203.1, the county financial officer shall distribute proceeds collected by the county pursuant to this section as follows:

(1) If the restitution judgment has been satisfied, but the surcharge remains outstanding, all amounts paid by the defendant shall be kept by the county and applied to the surcharge.

(2) If the surcharge has been satisfied, but the restitution judgment has not been satisfied, all amounts submitted to the county shall be remitted to the victim.

(3) If neither judgment has been satisfied, the county shall remit 70 percent of the amounts collected to the victim. Those amounts shall be credited to the restitution judgment. The remaining 30 percent shall be retained by the county and credited toward the surcharge.

(v) Neither this section, nor the amendments to Section 12022.6 of the Penal Code enacted pursuant to Chapter 104 of the Statutes of 1992, are intended to lessen or otherwise mitigate sentences that could otherwise be imposed under any law in effect when the offense was committed.

(w) For the purpose of this section, a county may designate an appropriate employee of the county probation department, the department revenue, or any other analogous county department to act as the county financial officer pursuant to this section.

(x) This act shall be known as the Economic Crime Act of 1992.

LEGISLATIVE NOTES

"Section 1. The Legislature finds and declares that major economic or "white collar" crime is an increasing threat to California's economy and the well-being of its citizens. The Legislature intends to deter that crime by ensuring that every offender, without exception, serves at least some time in jail and by requiring the offenders to divert a portion of their future resources to the restitution to their victims.

"White collar criminals granted probation too often complete their probation without having

compensated their victims or society.

"Probation accompanied by a restitution order is often ineffective because county financial officers are often unaware of the income and assets enjoyed by white collar offenders. Local agencies lack the resources to obtain that information and sometimes set payment schedules for restitution too low. Officials responsible for enforcement are often too overburdened to pursue hidden assets. Thus, it is the Legislature's intent that the financial reporting requirements of this act be utilized to achieve satisfactory disclosure to permit an appropriate restitution order.

"White collar criminal investigations and prosecutions are unusually expensive. These high costs sometimes discourage vigorous enforcement of white collar crime laws by local agencies. Thus, it is necessary to require white collar offenders to assist in funding this enforcement activity.

"It is the intent of the Legislature to have this legislation accomplish the punishment, deterrent, and rehabilitative goals contemplated by the United States Supreme Court as stated in Kelly v. Robinson, 479 U.S. 36."

"Sec. 3. This act shall remain in effect until January 1, 1998, on which date it shall be repealed. "Sec. 4. This act applies to any crime committed on or after January 1, 1993."

§1203.047. Conviction of computer crime; probation

A person convicted of a violation of paragraph (1), (2), (4), or (5) of subdivision (c) of Section 502, or of a felony violation of paragraph (3), (6), (7), or (8) of subdivision (c) of Section 502, or a violation of subdivision (b) of Section 502.7 may be granted probation, but, except in unusual cases where the ends of justice would be better served by a shorter period, the period of probation shall not be less than three years and the following terms shall be imposed. During the period of probation, that person shall not accept employment where that person would use a computer connected by any means to any other computer, except upon approval of the court and notice to and opportunity to be heard by the prosecuting attorney, probation department, prospective employer, and the convicted person. Court approval shall not be given unless the court finds that the proposed employment would not pose a risk to the public.

§1203.048. Property damage limitation; probation; conviction of computer crime

(a) Except in unusual cases where the interests of justice would best be served if the person is granted probation, probation shall not be granted to any person convicted of a violation of Section 502 or subdivision (b) of Section 502.7 involving the taking of or damage to property with a value exceeding one hundred thousand dollars ($100,000).

(b) The fact that the value of the property taken or damaged was an amount exceeding one hundred thousand dollars ($100,000) shall be alleged in the accusatory pleading, and either admitted by the defendant in open court, or found to be true by the jury trying the issue of guilt or by the court where guilt is established by plea of guilt or nolo contendere or by trial by the court sitting without a jury.

(c) When probation is granted, the court shall specify on the record and shall enter on the minutes the circumstances indicating that the interests of justice would best be served by such a disposition.

ANNOTATED CALIFORNIA CODES

PENAL CODE
PART 2. OF CRIMINAL PROCEDURE
TITLE 12. SPECIAL PROCEEDINGS OF A CRIMINAL NATURE
CHAPTER 3. SEARCH WARRANTS

§1524. Issuance; grounds; special master

. . .

(f) As used in this section "documentary evidence" includes, but is not limited to, writings, documents, blueprints, drawings, photographs, computer printouts, microfilms, X-rays, files, diagrams, ledgers, books, tapes, audio and video recordings, films or papers of any type or description.

. . .

ANNOTATED CALIFORNIA CODES

PENAL CODE
PART 3. OF IMPRISONMENT AND THE DEATH PENALTY
TITLE 1. IMPRISONMENT OF MALE PRISONERS IN STATE PRISONS
CHAPTER 5. EMPLOYMENT OF PRISONERS
ARTICLE 1. EMPLOYMENT OF PRISONERS GENERALLY

§2702. Prisoners convicted of computer crimes; access to department computer system

No person imprisoned after conviction of a violation of Section 502 or of subdivision (b) of Section 502.7 shall be permitted to work on or have access to any computer system of the department.

ANNOTATED CALIFORNIA CODES

PENAL CODE
PART 1. OF CRIMES AND PUNISHMENTS
TITLE 13. OF CRIMES AGAINST PROPERTY
CHAPTER 5. LARCENY [THEFT]

§484j. Publication of access card, number or code with intent to defraud another

Any person who publishes the number or code of an existing, canceled, revoked, expired or nonexistent access card, personal identification number, computer password, access code, debit card number, bank account number, or the numbering or coding which is employed in the issuance of access cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful charge, or with intent to defraud or aid another in defrauding, is guilty of a misdemeanor. As used in this section, "publishes" means the communication of information to any one or more persons, either orally, in person or by telephone, radio or television, or on a computer network or computer bulletin board, or in a writing of any kind, including without limitation a letter or memorandum, circular or handbill, newspaper or magazine article, or book.

§496. Receiving stolen property

(a) Receiving; knowledge; concealment; punishment. Every person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained, is punishable by imprisonment in a state prison, or in a county jail for not more than one year . However, if the district attorney or the grand jury determines that this action would be in the interests of justice, the district attorney or the grand jury, as the case may be, may, if the value of the property does not exceed four hundred dollars ($400), specify in the accusatory pleading that the offense shall be a misdemeanor, punishable only by imprisonment in a county jail not exceeding one year. A principal in the actual theft of the property may be convicted pursuant to this section. However, no person may be convicted both pursuant to this section and of the theft of the same property.

(b) Swap meet vendors; secondhand dealers; inquiry; presumption. Every swap meet vendor, as defined in Section 21661 of the Business and Professions Code, and every person whose principal business is dealing in, or collecting, used or secondhand merchandise or personal property, and every agent, employee, or representative of that person, who buys or receives any property that has been stolen or obtained in any manner constituting theft or extortion, under circumstances that should cause the person, agent, employee, or representative to make reasonable inquiry to ascertain that the person from whom the property was bought or received had the legal right to sell or deliver it, without making a reasonable inquiry, shall be presumed to have bought or received the property knowing it to have been so stolen or obtained. This presumption may, however, be rebutted by proof.

(c) Swap meet vendors; secondhand dealers; inquiry; burden of proof. When in a prosecution under this section it shall appear from the evidence that the defendant was a swap meet vendor or that the defendant's principal business was as set forth in subdivision (b), that the defendant bought, received, or otherwise obtained, or concealed,

withheld, or aided in concealing or withholding, from the owner, any property that had been stolen or obtained in any manner constituting theft or extortion, and that the defendant bought, received, obtained, concealed, or withheld that property under circumstances that should have caused him or her to make reasonable inquiry to ascertain that the person from whom he or she bought, received, or obtained the property had the legal right to sell or deliver it to him or her, then the burden shall be upon the defendant to show that before buying, receiving, or otherwise obtaining the property, he or she made a reasonable inquiry to ascertain that the person selling or delivering the same to him or her had the legal right to sell or deliver it.

(d) Damages and costs. Any person who has been injured by a violation of subdivision (a) may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees.

(e) Attempts; penalties. Notwithstanding Section 664, any attempt to commit any act prohibited by this section, except an offense specified in the accusatory pleading as a misdemeanor, is punishable by imprisonment in a state prison, or in a county jail for not more than one year.

§499c. Trade secrets; theft; solicitation or bribery to acquire; punishment; defenses

(a) As used in this section:

(1) "Access" means to approach, a way or means of approaching, nearing, admittance to, including to instruct, communicate with, store information in, or retrieve information from a computer system or computer network.

(2) "Article" means any object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, micro-organism, blueprint, map, or tangible representation of computer program or information, including both human and computer readable information and information while in transit.

(3) "Benefit" means gain or advantage, or anything regarded by the beneficiary as gain or advantage, including benefit to any other person or entity in whose welfare he is interested.

(4) "Computer system" means a machine or collection of machines, one or more of which contain computer programs and information, that performs functions, including, but not limited to, logic, arithmetic, information storage and retrieval, communications, and control.

(5) "Computer network" means an interconnection of two or more computer systems.

(6) "Computer program" means an ordered set of instructions or statements, and related information that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(7) "Copy" means any facsimile, replica, photograph or other reproduction of an article, and any note, drawing or sketch made of or from an article.

(8) "Representing" means describing, depicting, containing, constituting, reflecting or recording.

(9) "Trade secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, computer program or information stored in a computer, information in transit, or improvement which is secret and is not generally available to the public, and which gives one who uses it an advantage over competitors who do not know of or use the trade secret; and a trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.

(b) Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his or her own use or to the use of another, does any of the following:

(1) Steals, takes, carries away, or uses without authorization a trade secret.

(2) Fraudulently appropriates any article representing a trade secret entrusted to him.

(3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.

(4) Having obtained access to the article through a relationship of trust and confidence, without authority and in breach of the obligations created by such relationship makes or causes to be made, directly from and in the presence of the article, a copy of any article representing a trade secret.

(c) Every person who promises or offers or gives, or conspires to promise or offer to give, to any present or former agent, employee or servant of another a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his or her present or former principal, employer or master, to any person not authorized by such owner to receive or acquire the same and every person who being a present or former agent, employee, or servant, solicits, accepts, receives or takes a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his or her present or former principal, employer or master, to any person not authorized by such owner to receive or acquire the same is punishable by imprisonment in the state prison, or in a county jail not exceeding one year, or by fine not exceeding five thousand dollars ($5,000), or by both such fine and such imprisonment.

(d) In a prosecution for a violation of this section it shall be no defense that the person so charged, returned or intended to return the article.

§502.01. Forfeiture of property used in committing computer crimes; redemption of interests; application to minors; distribution of proceeds

(a) As used in this section:

(1) "Property subject to forfeiture" means any property of the defendant that is a computer, computer system, or computer network, and any software or data residing thereon, if the computer, computer system, or computer network was used in committing a violation of subdivision (c) of Section 502 or a violation of Section 502.7 or was used as a repository for the storage of software or data obtained in violation of those provisions. If the defendant is a minor, it also includes property of the parent or guardian of the defendant.

(2) "Sentencing court" means the court sentencing a person found guilty of violating subdivision (c) of Section 502 or a violation of Section 502.7 or, in the case of a minor found to be a person described in Section 602 of the Welfare and Institutions Code because of a violation of those provisions, the juvenile court.

(3) "Interest" means any property interest in the property subject to forfeiture.

(4) "Security interest" means an interest that is a lien, mortgage, security interest, or interest under a conditional sales contract.

(b) The sentencing court shall, upon petition by the prosecuting attorney, at any time following sentencing, or by agreement of all parties, at the time of sentencing, conduct a hearing to determine whether any property or property interest is subject to forfeiture under this section. At the forfeiture hearing, the prosecuting attorney shall have the burden of establishing, by a preponderance of the evidence, that the property or property interests are subject to forfeiture. The prosecuting attorney may retain seized property that may be subject to forfeiture until the sentencing hearing.

(c) Prior to the commencement of a forfeiture proceeding, the law enforcement agency seizing the property subject to forfeiture shall make an investigation as to any person other than the defendant who may have an interest in it. At least 30 days before the hearing to determine whether the property should be forfeited, the prosecuting agency shall send notice of the hearing to any person who may have an interest in the property that arose before the seizure. A person claiming an interest in the property shall file a motion for the redemption of that interest at least 10 days before the hearing on forfeiture, and a copy of the motion to the prosecuting agency and to the probation department. If a motion to redeem an interest has been filed, the sentencing court shall hold a hearing to identify all persons who possess valid interests in the property. No person shall hold a valid interest in the property if, by a preponderance of the evidence, the prosecuting agency shows that the person knew or should have known that the property was being used in violation of subdivision (c) of Section 502 or Section 502.7, and that the person did not take reasonable steps to prevent that use, or if the interest is a security interest, the person knew or should have known at the time that the security

interest was created that the property would be used for such a violation.

(d) If the sentencing court finds that a person holds a valid interest in the property, the following provisions shall apply:

(1) The court shall determine the value of the property.

(2) The court shall determine the value of each valid interest in the property.

(3) If the value of the property is greater than the value of the interest, the holder of the interest shall be entitled to ownership of the property upon paying the court the difference between the value of the property and the value of the valid interest. If the holder of the interest declines to pay the amount determined under paragraph (2), the court may order the property sold and designate the prosecutor or any other agency to sell the property. The designated agency shall be entitled to seize the property and the holder of the interest shall forward any documentation underlying the interest, including any ownership certificates for that property, to the designated agency. The designated agency shall sell the property and pay the owner of the interest the proceeds, up to the value of that interest.

(4) If the value of the property is less than the value of the interest, the designated agency shall sell the property and pay the owner of the interest the proceeds, up to the value of that interest.

(e) If the defendant was a minor at the time of the offense, this subdivision shall apply to property subject to forfeiture that is the property of the parent or guardian of the minor.

(1) The prosecuting agency shall notify the parent or guardian of the forfeiture hearing at least 30 days before the date set for the hearing.

(2) The computer shall not be subject to forfeiture if the parent or guardian files a signed statement with the court at least 10 days before the date set for the hearing that the minor shall not have access to any computer owned by the parent or guardian for two years after the date on which the minor is sentenced.

(3) If the minor is convicted of a violation of subdivision (c) of Section 502 or Section 502.7 within two years after the date on which the minor is sentenced, and the violation involves a computer owned by the parent or guardian, the original property subject to forfeiture, and the property involved in the new offense, shall be subject to forfeiture notwithstanding paragraph (2).

(f) If the defendant is found to have the only valid interest in the property subject to forfeiture, it shall be distributed as follows:

(1) First, to the victim, if the victim elects to take the property as full or partial restitution for injury, victim expenditures, or compensatory damages, as defined in paragraph (1) of subdivision (e) of Section 502. If the victim elects to receive

the property under this paragraph, the value of the property shall be determined by the court and that amount shall be credited against the restitution owed by the defendant. The victim shall not be penalized for electing not to accept the forfeited property in lieu of full or partial restitution.

(2) Second, at the discretion of the court, to one or more of the following agencies or entities:

(A) The prosecuting agency.
(B) The public entity of which the prosecuting agency is a part.
(C) The public entity whose officers or employees conducted the investigation resulting in forfeiture.
(D) Other state and local public entities, including school districts.
(E) Nonprofit charitable organizations.

(g) If the property is to be sold, the court may designate the prosecuting agency or any other agency to sell the property at auction. The proceeds of the sale shall be distributed by the court as follows:

(1) To the bona fide or innocent purchaser or encumbrancer, conditional sales vendor, or mortgagee of the property up to the amount of his or her interest in the property, if the court orders a distribution to that person.

(2) The balance, if any, to be retained by the court, subject to the provisions for distribution under subdivision (f).

§502.7. Obtaining telephone or telegraph services by fraud

(a) Any person who, knowingly, willfully, and with intent to defraud a person providing telephone or telegraph service, avoids or attempts to avoid, or aids, abets or causes another to avoid the lawful charge, in whole or in part, for telephone or telegraph service by any of the following means is guilty of a misdemeanor or a felony, as provided in subdivision (f):

(1) By charging the service to an existing telephone number or credit card number without the authority of the subscriber thereto or the lawful holder thereof.

(2) By charging the service to a nonexistent telephone number or credit card number, or to a number associated with telephone service which is suspended or terminated, or to a revoked or canceled (as distinguished from expired) credit card number, notice of the suspension, termination, revocation, or cancellation of the telephone service or credit card having been given to the subscriber thereto or the holder thereof .

(3) By use of a code, prearranged scheme, or other similar stratagem or device whereby the person, in effect, sends or receives information.

(4) By rearranging, tampering with, or making connection with telephone or telegraph facilities or equipment, whether physically, electrically, acoustically, inductively, or otherwise, or by using telephone or telegraph service with knowledge or reason to believe that the rearrangement, tampering, or connection existed at the time of the use .

(5) By using any other deception, false pretense, trick, scheme, device, or means.

(b) Any person who (1) makes, possesses, sells, gives, or otherwise transfers to another, or offers or advertises any instrument, apparatus, or device with intent to use it or with knowledge or reason to believe it is intended to be used to avoid any lawful telephone or telegraph toll charge or to conceal the existence or place of origin or destination of any telephone or telegraph message; or (2) sells, gives, or otherwise transfers to another or offers, or advertises plans or instructions for making or assembling an instrument, apparatus, or device described in paragraph (1) of this subdivision with knowledge or reason to believe that they may be used to make or assemble the instrument, apparatus, or device is guilty of a misdemeanor or a felony, as provided in subdivision (f).

(c) Any person who publishes the number or code of an existing, canceled, revoked, expired, or nonexistent credit card, or the numbering or coding which is employed in the issuance of credit cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful telephone or telegraph toll charge is guilty of a misdemeanor. The provisions of subdivision (f) shall not apply to this subdivision. As used in this section, "publishes" means the communication of information to any one or more persons, either orally, in person or by telephone, radio, or television, or in a writing of any kind, including without limitation a letter or memorandum, circular or handbill, newspaper, or magazine article, or book.

(d) Subdivision (a) applies when the telephone or telegraph communication involved either originates or terminates, or both originates and terminates, in this state, or when the charges for service would have been billable, in normal course, by a person providing telephone or telegraph service in this state, but for the fact that the charge for service was avoided, or attempted to be avoided, by one or more of the means set forth in subdivision (a).

(e) Jurisdiction of an offense under this section is in the jurisdictional territory where the telephone call or telegram involved in the offense originates or where it terminates, or the jurisdictional territory to which the bill for the service is sent or would have been sent but for the fact that the service was obtained or attempted to be obtained by one or more of the means set forth in subdivision (a).

(f) If the total value of all telephone or telegraph services obtained in violation of this section aggregates over four hundred dollars ($400) within any period of twelve (12) consecutive months during the three years immediately prior to the time the indictment is found or the case is certified to the superior court, or prior to the time the information is filed, or if the defendant has previously been convicted of an offense in excess of four hundred dollars ($400) under this section or of an offense in excess of four hundred dollars ($400) under the laws of another state or of the United States which would have

been an offense under this section if committed in this state, a person guilty of such offense is punishable by imprisonment in the county jail not exceeding one year, by a fine not exceeding one thousand dollars ($1,000), or both, or by imprisonment in the state prison, by a fine not exceeding ten thousand dollars ($10,000), or both.

(g) Any instrument, apparatus, device, plans, instructions, or written publication described in subdivision (b) or (c) may be seized under warrant or incident to a lawful arrest, and, upon the conviction of a person for a violation of subdivision (a), (b), or (c), the instrument, apparatus, device, plans, instructions, or written publication may be destroyed as contraband by the sheriff of the county in which the person was convicted or turned over to the person providing telephone or telegraph service in the territory in which it was seized.

(h) Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in this section or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of this section shall be subject to forfeiture.

§502. Unauthorized access to computers, computer systems and computer data

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data. The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation which does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation which results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the

county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (8) of subdivision (c) is punishable as follows:

(A) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars ($250).

(B) For any violation which results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation which results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by

the defendant, which is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture , as specified in Section 502.01.

(h) (1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed an accumulated total of one hundred dollars ($100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision

(h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

ANNOTATED CALIFORNIA CODES

PENAL CODE
PART 1. OF CRIMES AND PUNISHMENTS
TITLE 13. OF CRIMES AGAINST PROPERTY
CHAPTER 8. FALSE PERSONATION AND CHEATS

§537e. Removal or alteration of manufacturer's serial number or identification mark; purchase, sale, possession, etc.; disposition

(a) Any person who knowingly buys, sells, receives, disposes of, conceals, or has in his or her possession any personal property from which the manufacturer's serial number or any other distinguishing number or identification mark has been removed, defaced, covered, altered, or destroyed, is guilty of a public offense, punishable as follows:

(1) If the value of the property does not exceed four hundred dollars ($400), by imprisonment in the county jail not exceeding six months.

(2) If the value of the property exceeds four hundred dollars ($400), by imprisonment in the county jail not exceeding one year.

(3) If the property is an integrated computer chip or panel of a value of four hundred dollars ($400) or more, by imprisonment in the state prison for 16 months, or 2 or 3 years or by imprisonment in a county jail not exceeding one year. For purposes of this subdivision, "personal property" includes, but is not limited to, the following:

(1) Any television, radio, recorder, phonograph, telephone, piano, or any other musical instrument or sound equipment.

(2) Any washing machine, sewing machine, vacuum cleaner, or other household appliance or furnishings.

(3) Any typewriter, adding machine, dictaphone, or any other office equipment or furnishings.

(4) Any computer, printed circuit, integrated chip or panel, or other part of a computer.

(5) Any tool or similar device, including any technical or scientific equipment.

(6) Any bicycle, exercise equipment, or any other entertainment or recreational equipment.

(7) Any electrical or mechanical equipment, contrivance, material, or piece of apparatus or equipment.

(8) Any clock, watch, watch case, or watch movement.

(9) Any vehicle or vessel, or any component part thereof.

(b) When property described in subdivision (a) comes into the custody of a peace officer it shall become subject to the provision of Chapter 12 (commencing with Section 1407), Title 10 of Part 2, relating to the disposal of stolen or embezzled property. Property subject to this section shall be considered stolen or embezzled property for the purposes of that chapter, and prior to being disposed of, shall have an identification mark imbedded or engraved in, or permanently affixed to it.

(c) This section does not apply to those cases or instances where any of the changes or alterations enumerated in subdivision (a) have been customarily made or done as an established practice in the ordinary and regular conduct of business, by the original manufacturer, or by his or her duly appointed direct representative, or under specific authorization from the original manufacturer.

COLORADO REVISED STATUTES ANNOTATED

TITLE 18. CRIMINAL CODE
ARTICLE 5.5. COMPUTER CRIME

§18-5.5-101. Definitions

As used in this article, unless the context otherwise requires:

(1) "Authorization" means the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section.

(2) "Computer" means an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

(10) To "use" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

§18-5.5-102. Computer crime

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to

defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than one hundred dollars, computer crime is a class 3 misdemeanor; if one hundred dollars or more but less than four hundred dollars, computer crime is a class 2 misdemeanor; if four hundred dollars or more but less than fifteen thousand dollars, computer crime is a class 5 felony; if fifteen thousand dollars or more, computer crime is a class 3 felony.

§18-5.5-102. Computer crime

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than three hundred dollars, computer crime is a class 2 misdemeanor; if three hundred dollars or more but less than ten thousand dollars, computer crime is a class 5 felony; if ten thousand dollars or more, computer crime is a class 3 felony.

§ 52-570b. Action for computer-related offenses

(a) Any aggrieved person who has reason to believe that any other person has been engaged, is engaged or is about to engage in an alleged violation of any provision of section 53a-251 may bring an action against such person and may apply to the superior court for: (1) An order temporarily or permanently restraining and enjoining the commencement or continuance of such act or acts; (2) an order directing restitution; or (3) an order directing the appointment of a receiver. Subject to making due provisions for the rights of innocent persons, a receiver shall have the power to sue for, collect, receive and take into his possession any property which belongs to the person who is alleged to have violated any provision of section 53a-251 and which may have been derived by, been used in or aided in any manner such alleged violation. Such property shall include goods and chattels, rights and credits, moneys and effects, books, records, documents, papers, choses in action, bills, notes and property of every description including all computer system equipment and data, and including property with which such property has been commingled if it cannot be identified in kind because of such commingling. The receiver shall also have the power to sell, convey and assign all of the foregoing and hold and dispose of the proceeds thereof under the direction of the court. Any person who has suffered damages as a result of an alleged violation of any provision of section 53a-251, and submits proof to the satisfaction of the court that he has in fact been damaged, may participate with general creditors in the distribution of the assets to the extent he has sustained out-of-pocket losses. The court shall have jurisdiction of all questions arising in such proceedings and may make such orders and judgments therein as may be required.

(b) The court may award the relief applied for or such other relief as it may deem appropriate in equity.

(c) Independent of or in conjunction with an action under subsection (a) of this section, any person who suffers any injury to person, business or property may bring an action for damages against a person who is alleged to have violated any provision of section 53a-251. The aggrieved person shall recover actual damages and damages for unjust enrichment not taken into account in computing damages for actual loss, and treble damages where there has been a showing of wilful and malicious conduct.

(d) Proof of pecuniary loss is not required to establish actual damages in connection with an alleged violation of subsection (e) of section 53a-251 arising from misuse of private personal data.

(e) In any civil action brought under this section, the court shall award to any aggrieved person who prevails, reasonable costs and reasonable attorney's fees.

(f) The filing of a criminal action against a person is not a prerequisite to the bringing of a civil action under this section against such person.

(g) A civil action may be brought under this section against the state or any political

subdivision thereof and the defense of governmental immunity shall not be available in any such action. The rights and liability of the state or any political subdivision thereof in each such action shall be coextensive with and shall equal the rights and liability of private persons in like circumstances.

(h) No civil action under this section may be brought but within three years from the date the alleged violation of section 53a-251 is discovered or should have been discovered by the exercise of reasonable diligence.

CONNECTICUT GENERAL STATUTES ANNOTATED

TITLE 53A. PENAL CODE
CHAPTER 952. PENAL CODE: OFFENSES
PART XXII. COMPUTER-RELATED OFFENSES

§53a-250. Definitions

For the purposes of this part and section 52-570b:

(1) "Access" means to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer network.

(2) "Computer" means a programmable, electronic device capable of accepting and processing data.

(3) "Computer network" means (A) a set of related devices connected to a computer by communications facilities, or (B) a complex of two or more computers, including related devices, connected by communications facilities.

(4) "Computer program" means a set of instructions, statements or related data that, in actual or modified form, is capable of causing a computer or computer system to perform specified functions.

(5) "Computer services" includes, but is not limited to, computer access, data processing and data storage.

(6) "Computer software" means one or more computer programs, existing in any form, or any associated operational procedures, manuals or other documentation.

(7) "Computer system" means a computer, its software, related equipment, communications facilities, if any, and includes computer networks.

(8) "Data" means information of any kind in any form, including computer software.

(9) "Person" means a natural person, corporation, trust, partnership, incorporated or unincorporated association and any other legal or governmental entity, including any state or municipal entity or public official.

(10) "Private personal data" means data concerning a natural person which a reasonable person would want to keep private and which is protectable under law.

(11) "Property" means anything of value, including data.

§53a-251. Computer crime

(a) Defined. A person commits computer crime when he violates any of the provisions of this section.

(b) Unauthorized access to a computer system. (1) A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized

to do so, he accesses or causes to be accessed any computer system without authorization.

(2) It shall be an affirmative defense to a prosecution for unauthorized access to a computer system that: (A) The person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, had authorized him to access; (B) the person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, would have authorized him to access without payment of any consideration; or (C) the person reasonably could not have known that his access was unauthorized.

(c) Theft of computer services. A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services.

(d) Interruption of computer services. A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.

(e) Misuse of computer system information. A person is guilty of the computer crime of misuse of computer system information when: (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization (A) alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system, or (B) intercepts or adds data to data residing within a computer system; or (3) he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection.

(f) Destruction of computer equipment. A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.

§53a-252. Computer crime in the first degree: Class B felony

(a) A person is guilty of computer crime in the first degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds ten thousand dollars.

(b) Computer crime in the first degree is a class B felony.

§53a-253. Computer crime in the second degree: Class C felony

(a) A person is guilty of computer crime in the second degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds five thousand dollars.

(b) Computer crime in the second degree is a class C felony.

§53a-254. Computer crime in the third degree: Class D felony

(a) A person is guilty of computer crime in the third degree when he commits computer crime as defined in section 53a-251 and (1) the damage to or the value of the property or computer services exceeds one thousand dollars or (2) he recklessly engages in conduct which creates a risk of serious physical injury to another person.

(b) Computer crime in the third degree is a class D felony.

§53a-255. Computer crime in the fourth degree: Class A misdemeanor

(a) A person is guilty of computer crime in the fourth degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services exceeds five hundred dollars.

(b) Computer crime in the fourth degree is a class A misdemeanor.

§53a-256. Computer crime in the fifth degree: Class B misdemeanor

(a) A person is guilty of computer crime in the fifth degree when he commits computer crime as defined in section 53a-251 and the damage to or the value of the property or computer services, if any, is five hundred dollars or less.

(b) Computer crime in the fifth degree is a class B misdemeanor.

§53a-257. Alternative fine based on defendant's gain

If a person has gained money, property or services or other consideration through the commission of any offense under section 53a-251, upon conviction thereof the court, in lieu of imposing a fine, may sentence the defendant to pay an amount, fixed by the court, not to exceed double the amount of the defendant's gain from the commission of such offense. In such case the court shall make a finding as to the amount of the defendant's gain from the offense and, if the record does not contain sufficient evidence to support such a finding, the court may conduct a hearing upon the issue. For the purpose of this section, "gain" means the amount of money or the value of property or computer services or other consideration derived.

§53a-258. Determination of degree of crime

Amounts included in violations of section 53a-251 committed pursuant to one scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the degree of the crime.

§53a-259. Value of property or computer services

(a) For the purposes of this part and section 52-570b, the value of property or computer services shall be: (1) The market value of the property or computer services at the time of the violation; or (2) if the property or computer services are unrecoverable, damaged or destroyed as a result of a violation of section 53a-251, the cost of reproducing or replacing the property or computer services at the time of the violation.

(b) When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be two hundred fifty dollars.

(c) Notwithstanding the provisions of this section, the value of private personal data shall be deemed to be one thousand five hundred dollars.

§53a-260. Location of offense

(a) In any prosecution for a violation of section 53a-251 the offense shall be deemed to have been committed in the town in which the act occurred or in which the computer system or part thereof involved in the violation was located.

(b) In any prosecution for a violation of section 53a-251 based upon more than one act in violation thereof, the offense shall be deemed to have been committed in any of the towns in which any of the acts occurred or in which a computer system or part thereof involved in a violation was located.

§53a-261. Jurisdiction

If any act performed in furtherance of the offenses set out in section 53a-251 occurs in this state or if any computer system or part thereof accessed in violation of section 53a-251 is located in this state, the offense shall be deemed to have occurred in this state.

DELAWARE CODE ANNOTATED

TITLE 11. CRIMES AND CRIMINAL PROCEDURE
PART I. DELAWARE CRIMINAL CODE
CHAPTER 5. SPECIFIC OFFENSES
SUBCHAPTER III. OFFENSES INVOLVING PROPERTY
SUBPART K. COMPUTER RELATED OFFENSES

§931 Definitions.

As used in this subpart:

(1) "Access" means to instruct, communicate with, store data in or retrieve data from a computer, computer system or computer network.

(2) "Computer" means a programmable, electronic device capable of accepting and processing data.

(3) "Computer network" means:

a. A set of related devices connected to a computer by communications facilities;

b. A complex of 2 or more computers, including related devices, connected by communications facilities; or

c. The communications transmission facilities and devices used to interconnect computational equipment, along with control mechanisms associated thereto.

(4) "Computer program" means a set of instructions, statements or related data that, in actual or modified form, is capable of causing a computer or computer system to perform specified functions.

(5) "Computer services" includes, but is not limited to, computer access, data processing and data storage.

(6) "Computer software" means 1 or more computer programs, existing in any form, or any associated operational procedures, manuals or other documentation.

(7) "Computer system" means a computer, its software, related equipment and communications facilities, if any, and includes computer networks.

(8) "Data" means information of any kind in any form, including computer software.

(9) "Person" means a natural person, corporation, trust, partnership, incorporated or unincorporated association and any other legal or governmental entity, including any state or municipal entity or public official.

(10) "Private personal data" means data concerning a natural person which a reasonable person would want to keep private and which is protectable under law.

(11) "Property" means anything of value, including data.

§932 Unauthorized access.

A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization.

§933 Theft of computer services.

A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services, computer software or data.

§934 Interruption of computer services.

A person is guilty of the computer crime of interruption of computer services when that person, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.

§935 Misuse of computer system information.

A person is guilty of the computer crime of misuse of computer system information when:

(1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system;

(2) That person intentionally or recklessly and without authorization:

a. Alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system; or

b. Interrupts or adds data to data residing within a computer system;

(3) That person knowingly receives or retains data obtained in violation of Subdivision (1) or (2) of this section; or

(4) That person uses or discloses any data which that person knows or believes was obtained in violation of subdivision (1) or (2) of this section.

§936 Destruction of computer equipment.

A person is guilty of the computer crime of destruction of computer equipment when that person, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.

§937 Penalties [Amendment effective with respect to crimes committed June 30, 1990, or thereafter].

(a) A person committing any of the crimes described in §§ 932-936 of this title is guilty in the first degree when the damage to or the value of the property or computer services affected exceeds $10,000.

Computer crime in the first degree is a class D felony.

(b) A person committing any of the crimes described in §§ 932-936 of this title is guilty in the second degree when the damage to or the value of the property or computer services affected exceeds $5,000.

Computer crime in the second degree is a class E felony.

(c) A person committing any of the crimes described in §§ 932-936 of this title is guilty in the third degree when:

(1) The damage to or the value of the property or computer services affected exceeds $1,000; or

(2) That person engages in conduct which creates a risk of serious physical injury to another person.

Computer crime in the third degree is a class F felony.

(d) A person committing any of the crimes described in §§ 932-936 of this title is guilty in the fourth degree when the damage to or the value of the property or computer services affected exceeds $500.

Computer crime in the fourth degree is a class G felony.

(e) A person committing any of the crimes described in §§ 932-936 of this title is guilty in the fifth degree when the damage to or the value of the property or computer services, if any, is $500 or less.

Computer crime in the fifth degree is a class A misdemeanor.

(f) Any person gaining money, property services or other consideration through the commission of any offense under this subpart, upon conviction, in lieu of having a fine imposed, may be sentenced by the court to pay an amount, fixed by the court, not to

exceed double the amount of the defendant's gain from the commission of such offense. In such case, the court shall make a finding as to the amount of the defendant's gain from the offense and, if the record does not contain sufficient evidence to support such a finding, the court may conduct a hearing upon the issue. For the purpose of this section, "gain" means the amount of money or the value of property or computer services or other consideration derived.

(g) Amounts included in violations of this subpart committed pursuant to 1 scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the degree of the crime.

(h) For the purposes of this subpart, the value of property or computer services shall be:

(1) The market value of the property or computer services at the time of the violation; or

(2) If the property or computer services are unrecoverable, damaged or destroyed as a result of a violation of this subpart, the cost of reproducing or replacing the property or computer services at the time of the violation.

When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be $250.

(i) Notwithstanding this section, the value of private personal data shall be deemed to be $500.

§938 Venue.

(a) In any prosecution for any violation of §§ 932-936 of this title, the offense shall be deemed to have been committed in the place at which the act occurred or in which the computer system or part thereof involved in the violation was located.

(b) In any prosecution for any violation of §§ 932-936 of this title based upon more than 1 act in violation thereof, the offense shall be deemed to have been committed in any of the places at which any of the acts occurred or in which a computer system or part thereof involved in a violation was located.

(c) If any act performed in furtherance of the offenses set out in §§ 932-936 of this title occurs in this State or in any computer system or part thereof accessed in violation of §§ 932-936 of this title is located in this State, the offense shall be deemed to have occurred in this State.

§939 Remedies of aggrieved persons.

(a) Any aggrieved person who has reason to believe that any other person has been engaged, is engaged or is about to engage in an alleged violation of any provision of §§ 932-936 of this title may bring an action against such person and may apply to the Court of

Chancery for:

(i) An order temporarily or permanently restraining and enjoining the commencement or continuance of such act or acts;

(ii) an order directing restitution; or

(iii) an order directing the appointment of a receiver.

Subject to making due provisions for the rights of innocent persons, a receiver shall have the power to sue for, collect, receive and take into his possession any property which belongs to the person who is alleged to have violated any provision of this subpart and which may have been derived by, been used in or aided in any manner such alleged violation. Such property shall include goods and chattels, rights and credits, moneys and effects, books, records, documents, papers, choses in action, bills, notes and property of every description including all computer system equipment and data, and including property with which such property has been commingled if it cannot be identified in kind because of such commingling. The receiver shall also have the power to sell, convey and assign all of the foregoing and hold and dispose of the proceeds thereof under the direction of the Court. Any person who has suffered damages as a result of an alleged violation of any provision of §§ 932-936 of this title, and submits proof to the satisfaction of the Court that he has in fact been damaged, may participate with general creditors in the distribution of the assets to the extent he has sustained out-of-pocket losses. The Court shall have jurisdiction of all questions arising in such proceedings and may make such orders and judgments therein as may be required.

(b) The Court may award the relief applied for or such other relief as it may deem appropriate in equity.

(c) Independent of or in conjunction with an action under subsection (a) of this section, any person who suffers any injury to person, business or property may bring an action for damages against a person who is alleged to have violated any provision of §§ 932-936 of this title. The aggrieved person shall recover actual damages and damages for unjust enrichment not taken into account in computing damages for actual loss and treble damages where there has been a showing of wilful and malicious conduct.

(d) Proof of pecuniary loss is not required to establish actual damages in connection with an alleged violation of s 935 of this title arising from misuse of private personal data.

(e) In any civil action brought under this section, the Court shall award to any aggrieved person who prevails reasonable costs and reasonable attorney's fees.

(f) The filing of a criminal action against a person is not a prerequisite to the bringing of a civil action under this section against such person.

(g) No civil action under this section may be brought but within 3 years from the date the alleged violation of §§ 932-936 of this title is discovered or should have been discovered by the exercise of reasonable diligence.

FLORIDA STATUTES ANNOTATED

TITLE XLVI. CRIMES
CHAPTER 815. COMPUTER-RELATED CRIMES

REFERENCES

Civil remedies for criminal practices act, criminal activities to which provisions applicable, see § 772.102.

815.01. Short title

The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

815.02. Legislative intent

The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

815.03. Definitions

As used in this chapter, unless the context clearly indicates otherwise:

(1) "Intellectual property" means data, including programs.

(2) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(3) "Computer" means an internally programmed, automatic device that performs data processing.

(4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Property" means anything of value as defined in § 812.011 [FN1PP] and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

815.04. Offenses against intellectual property

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in § 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the

second degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

815.05. Offenses against computer equipment or supplies

(1)(a) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in § 775.082 or § 775.083.

2. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

(2)(a) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in § 775.082 or § 775.083.

2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

815.06. Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with

another commits an offense against computer users.

(2)(a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

(b) If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

815.07. This chapter not exclusive

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

FLORIDA STATUTES ANNOTATED

TITLE XLVI. CRIMES

CHAPTER 895. OFFENSES CONCERNING RACKETEERING AND ILLEGAL DEBTS

895.02. Definitions

As used in §§ 895.01-895.08, the term:

(1) "Racketeering activity" means to commit, to attempt to commit, to conspire to commit, or to solicit, coerce, or intimidate another person to commit:

(a) Any crime which is chargeable by indictment or information under the following provisions of the Florida Statutes:

. . .

20. Chapter 815, relating to computer-related crimes.

21. Chapter 817, relating to fraudulent practices, false pretenses, fraud generally, and credit card crimes.

. . .

(b) Any conduct defined as "racketeering activity" under 18 U.S.C. § 1961(1).

(2) "Unlawful debt" means any money or other thing of value constituting principal or interest of a debt that is legally unenforceable in this state in whole or in part because the debt was incurred or contracted:

(a) In violation of any one of the following provisions of law:

1. Section 550.24, § 550.35, or § 550.36, relating to dogracing, horseracing, and jai alai frontons.

2. Section 551.09, relating to jai alai frontons.

3. Chapter 687, relating to interest and usury.

4. Section 849.09, § 849.14, § 849.15, § 849.23, § 849.24, [FN1PP] or § 849.25, relating to gambling.

(b) In gambling activity in violation of federal law or in the business of lending money at a rate usurious under state or federal law.

(3) "Enterprise" means any individual, sole proprietorship, partnership, corporation, business trust, union chartered under the laws of this state, or other legal entity, or any unchartered union, association, or group of individuals associated in fact although not a legal entity; and it includes illicit as well as licit enterprises and governmental, as well as other, entities.

(4) "Pattern of racketeering activity" means engaging in at least two incidents of

racketeering conduct that have the same or similar intents, results, accomplices, victims, or methods of commission or that otherwise are interrelated by distinguishing characteristics and are not isolated incidents, provided at least one of such incidents occurred after the effective date of this act and that the last of such incidents occurred within 5 years after a prior incident of racketeering conduct.

(5) "Documentary material" means any book, paper, document, writing, drawing, graph, chart, photograph, phonorecord, magnetic tape, computer printout, other data compilation from which information can be obtained or from which information can be translated into usable form, or other tangible item.

(6) "RICO lien notice" means the notice described in § 895.05(12) or in § 895.07.

(7) "Investigative agency" means the Department of Legal Affairs, the Office of Statewide Prosecution, or the office of a state attorney.

(8) "Beneficial interest" means any of the following:

(a) The interest of a person as a beneficiary under a trust established pursuant to § 689.07 or § 689.071 in which the trustee for the trust holds legal or record title to real property;

(b) The interest of a person as a beneficiary under any other trust arrangement pursuant to which a trustee holds legal or record title to real property for the benefit of such person; or

(c) The interest of a person under any other form of express fiduciary.

CODE OF GEORGIA

TITLE 16. CRIMES AND OFFENSES
CHAPTER 9. FORGERY AND FRAUDULENT PRACTICES
ARTICLE 6. COMPUTER SYSTEMS PROTECTION

16-9-90 Short title.

This article may be cited as the "Georgia Computer Systems Protection Act." (Code 1981, § 1.)

16-9-91 Legislative findings.

The General Assembly finds that:

(1) Computer related crime is a growing problem in the government and in the private sector;

(2) Such crime occurs at great cost to the public, since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) The opportunities for computer related crimes in state programs, and in other entities which operate within the state, through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets are great;

(4) Computer related crime operations have a direct effect on state commerce;

(5) Liability for computer crimes should be imposed on all persons, as that term is defined in this title; and

(6) The prosecution of persons engaged in computer related crime is difficult under previously existing Georgia criminal statutes.

(Code 1981, § 16-9-91, enacted by Ga. L. 1991, p. 1045, § 1.) Code, § 16-9-91 GA ST § 16-9-91

16-9-92 Definitions.

As used in this article, the term:

(1) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device or system performing computer operations with or on data and includes any data storage facility or communications facility directly related to or operating in conjunction with such device; but such term does not include an automated typewriter or typesetter, portable hand-held calculator, household appliance, or other similar device that is not used to communicate with or to manipulate any other computer.

(2) "Computer network" means a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the communications facilities.

(3) "Computer operation" means computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording, reproducing, handling, or utilizing any form of data for business, scientific, control, or other purposes.

(4) "Computer program" means one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term "computer program" shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form.

(5) "Data" includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(6) "Financial instruments" includes any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism, or marketable security, or any computer representation thereof.

(7) "Property" includes computers, computer networks, computer programs, data, financial instruments, and services.

(8) "Services" includes computer time or services or data processing services.

(9) "Use" includes causing or attempting to cause:

(A) A computer or computer network to perform or to stop performing computer operations;

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

(C) A person to put false information into a computer.

(10) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

(11) "Without authority" includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

(Code 1981, § 16-9-92, enacted by Ga. L. 1991, p. 1045, § 1; Ga. L. 1992, p. 6, § 16.)

16-9-93 Computer crimes defined; exclusivity of article; civil remedies; criminal penalties.

(a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

(f) Article not Exclusive. The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this article.

(g) Civil Relief; Damages.

(1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

(h) Criminal Penalties.

(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

Note: For an update of crimes and offenses for which the Georgia Crime Information Center is authorized to collect and file identifying data, see 1991 Op. Att'y Gen. No. 91-35.

16-9-94 Venue.

For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

(1) In the county of the principal place of business in this state of the owner of a computer, computer network, or any part thereof;

(2) In any county in which any person alleged to have violated any provision of this article had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation;

(3) In any county in which any act was performed in furtherance of any transaction which violated this article; and

(4) In any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

HAWAII REVISED STATUTES ANNOTATED

DIVISION 5. CRIMES AND CRIMINAL PROCEEDINGS
TITLE 37. HAWAII PENAL CODE
CHAPTER 708. Offenses Against Property Rights
(PART IX.) [NEW] COMPUTER CRIME

Definitions.

As used in this part, unless the context otherwise requires:

"Access" means to gain entry to or communicate with a computer, computer system, or computer network.

"Computer" means any device which performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a computer system or computer network.

"Computer equipment" or "hardware" means central processing units, microprocessors, data storage and other computer memory devices, and computer terminals or similar devices.

"Computer network" means two or more computer systems connected so as to permit the exchange or sharing of data between or among them.

"Computer program" or "software" means a set of computer-readable instructions or statements which, when executed by a computer system, causes the computer system or the computer network to which it is connected to perform computer services.

"Computer services" means data input, data output, data processing, or data storage by or in a computer system or computer network.

"Computer system" means computer equipment or hardware connected together and operating under the control of one or more computer programs.

"Data" means information stored in a computer system or on electronic media or processed in a computer system.

"Disruption" means any deviation from normal operations of any computer, computer system, or computer network.

"Injury" includes addition, alteration, damage, deletion, destruction, denial of access with respect to data in, or functions of, a computer system or computer network.

"Property" includes financial instruments, data, computer software, computer programs, documents associated with computer systems and computer programs, or copies, whether tangible or intangible, and data while in transit.

"Without authorization" means without the permission of or in excess of the permission of an owner, lessor, or rightful user or someone licensed or privileged by an owner, lessor, or rightful user to grant such permission.

NOTES

Loss of information stored in computer system or on computer disk cartridge, computer tape, or similar computer storage media as within coverage of liability policy. 85 A.L.R.4th 1048.

(§708-891). Computer fraud.

(1) A person commits the offense of computer fraud if:

(a) The person accesses or causes to be accessed any computer, computer system, computer network, or any of its parts with the intent of devising or executing any scheme or artifice to defraud; or

(b) The person accesses or causes to be accessed any computer, computer system, computer network, or any of its parts with the intent of obtaining money, property or services by means of embezzlement or false or fraudulent representations; or

(c) The person, without authorization, accesses or causes to be accessed any computer, computer system, computer network, or any of its parts with the intent of obtaining credit information on another person; or

(d) The person accesses or causes to be accessed any computer, computer system, computer network, or any of its parts with the intent of introducing or causing to be introduced false information to damage or enhance the credit rating of any person.

(2) Computer fraud is a class C felony.

(§708-892). Unauthorized computer use.

(1) A person commits the offense of unauthorized computer use if the person intentionally and without authorization accesses, alters, injures, disrupts, damages, or destroys any computer, computer system, computer network, computer program, computer software, or any data stored therein.

(2) Unauthorized computer use is a class C felony.

(§708-893). Entry without disruption.

(1) The court may dismiss a prosecution if, having regard to the nature of the conduct alleged and nature of the attendant circumstances, it finds that the defendant's conduct did not actually cause harm or damage to any computer, computer system, computer network, or any of its data or software.

(2) The court shall not dismiss a prosecution under section (1) without filing a written statement of its reasons.

(§712A-5). Property subject to forfeiture; exemption. [Repealed effective July 1, 1993.]

(1) The following is subject to forfeiture:

(a) Property described in a statute authorizing forfeiture;

(b) Property used or intended for use in the commission of, attempt to commit, or conspiracy to commit a covered offense, or which facilitated or assisted such activity;

(c) Any firearm which is subject to forfeiture under any other subsection of this section or which is carried during, visible, or used in furtherance of the commission, attempt to commit, or conspiracy to commit a covered offense, or any firearm found in proximity to contraband or to instrumentalities of an offense;

(d) Contraband, which shall be seized and summarily forfeited to the State without regard to the procedures set forth in this chapter;

(e) Any proceeds or other property acquired, maintained, or produced by means of or as a result of the commission of the covered offense;

(f) Any property derived from any proceeds which were obtained directly or indirectly from the commission of a covered offense;

(g) Any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over any enterprise which has been established, participated in, operated, controlled, or conducted in order to commit a covered offense;

(h) All books, records, bank statements, accounting records, microfilms, tapes, computer data, or other data which are used, intended for use, or which facilitated or assisted in the commission of a covered offense, or which document the use of the proceeds of a covered offense.

(2) Except that:

(a) Real property, or an interest therein, may be forfeited under the provisions of this chapter only in cases in which the covered offense is chargeable as a felony offense under State law;

(b) No property shall be forfeited under this chapter to the extent of an interest of an owner, by reason of any act or omission established by that owner to have been committed or omitted without the knowledge and consent of that owner.

(c) No conveyance used by any person as a common carrier in the transaction of a business as a common carrier is subject to forfeiture under this section unless it appears that the owner or other person in charge of the conveyance is a consenting party or privy to a violation of this chapter;

(d) No conveyance is subject to forfeiture under this section by reason of any act or omission established by the owner thereof to have been committed or omitted without the owner's knowledge or consent.

(e) A forfeiture of a conveyance encumbered by a bona fide security interest is subject to the interest of the secured party if the secured party neither had knowledge or nor consented to the act or omission.

IDAHO CODE

TITLE 18. CRIMES AND PUNISHMENTS
CHAPTER 22. COMPUTER CRIME

18-2201 Definitions.

As used in this chapter:

(1) To "access" means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means, but is not limited to, an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means, but is not limited to, the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two (2) or more interconnected computers.

(4) "Computer program" means, but is not limited to, a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means, but is not limited to, computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means, but is not limited to, a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(8) "Services" include, but are not limited to, computer time, data processing, and storage functions.

Note: The words in parentheses so appeared in the law as enacted.

18-2202 Computer crime.

(1) Any person who knowingly accesses, attempts to access or uses, or attempts to use any computer, computer system, computer network, or any part thereof for the purpose of: devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or committing theft; commits computer crime.

(2) Any person who knowingly and without authorization alters, damages, or destroys any computer, computer system, or computer network described in section 18-2201, Idaho Code, or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) Any person who knowingly and without authorization uses, accesses, or attempts to access any computer, computer system, or computer network described in section 18-2201, Idaho Code, or any computer software, program, documentation or data contained in such computer, computer system, or computer network, commits computer crime.

(4) A violation of the provisions of subsections (1) or (2) of this section shall be a felony. A violation of the provisions of subsection (3) of this section shall be a misdemeanor.

ILLINOIS COMPILED STATUTES ANNOTATED

CHAPTER 720. CRIMINAL OFFENSES
CRIMINAL CODE
ACT 5. CRIMINAL CODE OF 1961
TITLE III. SPECIFIC OFFENSES
PART C. OFFENSES DIRECTED AGAINST PROPERTY
ARTICLE 16D. COMPUTER CRIME

§16D-1. Short title.

This Article shall be known and may be cited as the "Computer Crime Prevention Law".

§16D-2. Definitions.

As used in this Article, unless the context otherwise indicates:

(a) "Computer" means a device that accepts, processes, stores, retrieves or outputs data, and includes but is not limited to auxiliary storage and telecommunications devices connected to computers.

(b) "Computer program" or "program" means a series of coded instructions or statements in a form acceptable to a computer which causes the computer to process data and supply the results of the data processing.

(c) "Data" means a representation of information, knowledge, facts, concepts or instructions, including program documentation, which is prepared in a formalized manner and is stored or processed in or transmitted by a computer. Data shall be considered property and may be in any form including but not limited to printouts, magnetic or optical storage media, punch cards or data stored internally in the memory of the computer.

(d) In addition to its meaning as defined in Section 15-1 of this Code, "property" means:

(1) electronic impulses;

(2) electronically produced data;

(3) confidential, copyrighted or proprietary information;

(4) private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transactions and telecommunications services or permit electronic fund transfers;

(5) software or programs in either machine or human readable form; or

(6) any other tangible or intangible item relating to a computer or any part thereof.

(e) "Access" means to use, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise utilize any services of a computer.

(f) "Services" includes but is not limited to computer time, data manipulation or storage functions.

(g) "Vital services or operations" means those services or operations required to provide, operate, maintain, and repair network cabling, transmission, distribution, or computer facilities necessary to ensure or protect the public health, safety, or welfare. Public health, safety, or welfare include, but are not limited to, services provided by medical personnel or institutions, fire departments, emergency services agencies, national defense contractors, armed forces or militia personnel, private and public utility companies, or law enforcement agencies.

§16D-3. Computer Tampering.

(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:

(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data;

(2) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains data or services;

(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and damages or destroys the computer or alters, deletes or removes a computer program or data;

(4) Inserts or attempts to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program".

(b) Sentence.

(1) A person who commits the offense of computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class B misdemeanor.

(2) A person who commits the offense of computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.

(3) A person who commits the offense of computer tampering as set forth in

subsection (a)(3) or subsection (a)(4) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense. (c) Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses.

NOTES

P.A. 86-762 made it a crime to insert or attempt to insert a program knowing that it will or may damage or destroy that computer or any other computer subsequently accessing or being accessed by that computer or alter or delete data and authorized the sufferor of such loss to maintain a civil action to obtain appropriate relief.

§16D-4. Aggravated Computer Tampering.

(a) A person commits aggravated computer tampering when he commits the offense of computer tampering as set forth in subsection (a)(3) of Section 16D-3 and he knowingly:

(1) causes disruption of or interference with vital services or operations of State or local government or a public utility; or

(2) creates a strong probability of death or great bodily harm to one or more individuals.

(b) Sentence.

(1) A person who commits the offense of aggravated computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class 3 felony.

(2) A person who commits the offense of aggravated computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class 2 felony.
1993 Main Volume Credit(s)

§16D-5. Computer Fraud.

(a) A person commits the offense of computer fraud when he knowingly:

(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data, for the purpose of devising or executing any scheme, artifice to defraud, or as part of a deception;

(2) Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme, artifice to defraud, or as part of a deception; or

(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection with any scheme, artifice to defraud, or as part of a deception.

(b) Sentence.

(1) A person who commits the offense of computer fraud as set forth in subsection (a)(1) of this Section shall be guilty of a Class 4 felony.

(2) A person who commits the offense of computer fraud as set forth in subsection (a)(2) of this Section shall be guilty of a Class 3 felony.

(3) A person who commits the offense of computer fraud as set forth in subsection (a)(3) of this Section shall:

(i) be guilty of a Class 4 felony if the value of the money, property or services is $1,000 or less; or

(ii) be guilty of a Class 3 felony if the value of the money, property or services is more than $1,000 but less than $50,000; or

(iii) be guilty of a Class 2 felony if the value of the money, property or services is $50,000 or more.

§16D-6. Forfeiture.

1. Any person who commits the offense of computer fraud as set forth in Section 16D-5 shall forfeit, according to the provisions of this Section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offense. Such person shall also forfeit any interest in, security, claim against, or contractual right of any kind which affords him a source of influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquired through computer fraud. Proceedings instituted pursuant to this Section shall be subject to and conducted in accordance with the following procedures:

(a) The sentencing court shall, upon petition by the prosecuting agency, whether it is the Attorney General or a State's Attorney, at any time following sentencing, conduct a hearing to determine whether any property or property interest is subject to forfeiture under this Section. At the forfeiture hearing the People of the State of Illinois shall have the burden of establishing, by a preponderance of the evidence, that the property or property interests are subject to such forfeiture.

(b) In any action brought by the People of the State of Illinois under this Section, the circuit courts of Illinois shall have jurisdiction to enter such restraining orders,

injunctions or prohibitions, or to take such other action in connection with any real, personal, or mixed property or other interest subject to forfeiture, as they shall consider proper.

(c) In any action brought by the People of the State of Illinois under this Section, wherein any restraining order, injunction or prohibition or any other action in connection with any property or interest subject to forfeiture under this Section is sought, the circuit court presiding over the trial of the person or persons charged with computer fraud shall first determine whether there is probable cause to believe that the person or persons so charged have committed the offense of computer fraud and whether the property or interest is subject to forfeiture pursuant to this Section. In order to make this determination, prior to entering any such order, the court shall conduct a hearing without a jury, where the People shall establish:

(1) probable cause that the person or persons so charged have committed the offense of computer fraud, and

(2) probable cause that any property or interest may be subject to forfeiture pursuant to this Section. Such hearing may be conducted simultaneously with a preliminary hearing if the prosecution is commenced by information or complaint, or by motion of the People at any stage in the proceedings. The court may enter a finding of probable cause at a preliminary hearing following the filing of an information charging the offense of computer fraud or the return of an indictment by a grand jury charging the offense of computer fraud as sufficient evidence of probable cause for purposes of this Section. Upon such a finding, the circuit court shall enter such restraining order, injunction or prohibition, or shall take such other action in connection with any such property or other interest subject to forfeiture under this Section as is necessary to insure that such property is not removed from the jurisdiction of the court, concealed, destroyed or otherwise disposed of by the owner or holder of that property or interest prior to a forfeiture hearing under this Section. The Attorney General or State's Attorney shall file a certified copy of such restraining order, injunction or other prohibition with the recorder of deeds or registrar of titles of each county where any such property of the defendant may be located. No such injunction, restraining order or other prohibition shall affect the rights of any bona fide purchaser, mortgagee, judgment creditor or other lienholder arising prior to the date of such filing. The court may, at any time, upon verified petition by the defendant, conduct a hearing to release all or portions of any such property or interest which the court previously determined to be subject to forfeiture or subject to any restraining order, injunction, prohibition or other action. The court may release such property to the defendant for good cause shown and within the sound discretion of the court.

(d) Upon conviction of a person under Section 16D-5, the court shall authorize the Attorney General to seize and sell all property or other interest declared forfeited

under this Act, unless such property is required by law to be destroyed or is harmful to the public. The court may order the Attorney General to segregate funds from the proceeds of such sale sufficient:

(1) to satisfy any order of restitution, as the court may deem appropriate;

(2) to satisfy any legal right, title, or interest which the court deems superior to any right, title, or interest of the defendant at the time of the commission of the acts which gave rise to forfeiture under this Section; or

(3) to satisfy any bona-fide purchaser for value of the right, title, or interest in the property who was without reasonable notice that the property was subject to forfeiture.

Following the entry of an order of forfeiture, the Attorney General shall publish notice of the order and his intent to dispose of the property. Within the 30 days following such publication, any person may petition the court to adjudicate the validity of his alleged interest in the property. After the deduction of all requisite expenses of administration and sale, the Attorney General shall distribute the proceeds of such sale, along with any moneys forfeited or seized as follows:

(1) 50% shall be distributed to the unit of local government whose officers or employees conducted the investigation into computer fraud and caused the arrest or arrests and prosecution leading to the forfeiture. Amounts distributed to units of local government shall be used for training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud. In the event, however, that the investigation, arrest or arrests and prosecution leading to the forfeiture were undertaken solely by a State agency, the portion provided hereunder shall be paid into the State Police Services Fund of the Illinois Department of State Police to be used for training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud.

(2) 50% shall be distributed to the county in which the prosecution and petition for forfeiture resulting in the forfeiture was instituted by the State's Attorney, and deposited in a special fund in the county treasury and appropriated to the State's Attorney for use in training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud. Where a prosecution and petition for forfeiture resulting in the forfeiture has been maintained by the Attorney General, 50% of the proceeds shall be paid into the Attorney General's Financial Crime Prevention Fund. Where the Attorney General and the State's Attorney have participated jointly in any part of the proceedings, 25% of the proceeds forfeited shall be paid to the county in which the prosecution and petition for forfeiture resulting in the forfeiture occurred, and 25% shall be paid to the Attorney General's Financial Crime

Prevention Fund to be used for the purposes as stated in this subsection.

2. Where any person commits a felony under any provision of this Code or another statute and the instrumentality used in the commission of the offense, or in connection with or in furtherance of a scheme or design to commit the offense, is a computer owned by the defendant or if the defendant is a minor, owned by his or her parents or legal guardian, the computer shall be subject to the provisions of this Section. However, in no case shall a computer, or any part thereof, be subject to the provisions of the Section if the computer accessed in the commission of the offense is owned or leased by the victim or an innocent third party at the time of the commission of the offense or if the rights of creditors, lienholders, or any person having a security interest in the computer at the time of the commission of the offense shall be adversely affected.

NOTES

P.A. 85-1042 substituted a reference to the State Police Services Fund for a reference to the Law Enforcement Services Fund.

§16D-7. Rebuttable Presumption--without authority.

In the event that a person accesses or causes to be accessed a computer, which access requires a confidential or proprietary code which has not been issued to or authorized for use by that person, a rebuttable presumption exists that the computer was accessed without the authorization of its owner or in excess of the authority granted.

ANNOTATED INDIANA CODE

TITLE 35. CRIMINAL LAW AND PROCEDURE
ARTICLE 43. OFFENSES AGAINST PROPERTY
CHAPTER 1. ARSON; MISCHIEF

35-43-1-4 Computer tampering

Sec. 4. (a) As used in this section:

"Computer network" and "computer system" have the meanings set forth in IC 35-43-2-3.

"Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

"Data" means a representation of information, facts, knowledge, concepts, or instructions that:

(1) may take any form, including computer printouts, magnetic storage media, punched cards, or stored memory;

(2) has been prepared or is being prepared; and

(3) has been processed, is being processed, or will be processed; in a computer system or computer network.

(b) A person who knowingly or intentionally alters or damages a computer program or data, which comprises a part of a computer system or computer network without the consent of the owner of the computer system or computer network commits computer tampering, a Class D felony.

ANNOTATED INDIANA CODE

TITLE 35. CRIMINAL LAW AND PROCEDURE
ARTICLE 43. OFFENSES AGAINST PROPERTY
CHAPTER 2. BURGLARY; TRESPASS

35-43-2-3 Computer trespass

Sec. 3. (a) As used in this section:

"Access" means to:

(1) approach;
(2) instruct;
(3) communicate with;
(4) store data in;
(5) retrieve data from; or
(6) make use of resources of;

a computer, computer system, or computer network.

"Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers.

"Computer system" means a set of related computer equipment, software, or hardware.

(b) A person who knowingly or intentionally accesses:

(1) a computer system;
(2) a computer network; or
(3) any part of a computer system or computer network; without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor.

ANNOTATED INDIANA CODE

TITLE 35. CRIMINAL LAW AND PROCEDURE
ARTICLE 43. OFFENSES AGAINST PROPERTY
CHAPTER 5. FORGERY AND OTHER DECEPTIONS

35-43-5-4 Fraud

Sec. 4. A person who:

(1) with intent to defraud, obtains property by:

(A) using a credit card, knowing that the credit card was unlawfully obtained or retained;

(B) using a credit card, knowing that the credit card is forged, revoked, or expired;

(C) using, without consent, a credit card that was issued to another person;

(D) representing, without the consent of the credit card holder, that the person is the authorized holder of the credit card; or

(E) representing that the person is the authorized holder of a credit card when the card has not in fact been issued;

(2) being authorized by an issuer to furnish property upon presentation of a credit card, fails to furnish the property and, with intent to defraud the issuer or the credit card holder, represents in writing to the issuer that the person has furnished the property;

(3) being authorized by an issuer to furnish property upon presentation of a credit card, furnishes, with intent to defraud the issuer or the credit card holder, property upon presentation of a credit card, knowing that the credit card was unlawfully obtained or retained or that the credit card is forged, revoked, or expired;

(4) not being the issuer, knowingly or intentionally sells a credit card;

(5) not being the issuer, receives a credit card, knowing that the credit card was unlawfully obtained or retained or that the credit card is forged, revoked, or expired;

(6) with intent to defraud, receives a credit card as security for debt;

(7) receives property, knowing that the property was obtained in violation of subdivision (1) of this section;

(8) with intent to defraud the person's creditor or purchaser, conceals, encumbers, or transfers property;

(9) with intent to defraud, damages property;

(10) knowingly and with intent to defraud, makes, utters, presents, or causes to be presented to an insurer, a claim statement that contains false, incomplete, or misleading information concerning the claim; or

(11) knowingly or intentionally:

(A) sells;

(B) rents;

(C) transports; or

(D) possesses;

a recording for commercial gain or personal financial gain that does not conspicuously display the true name and address of the manufacturer of the recording;

commits fraud, a Class D felony.

NOTES

Committing offense specified in this section and attempt, conspiracy or aiding and abetting to commit, defined as "racketeering activity", see section 35-45-6-1(d).

Consumer credit transactions, crimes and offenses, see section 24-4.5-5-301.

Sentence for class D felony, see section 35-50-2-7.

SELECTED LEGISLATIVE HISTORY

Theft of credit card, unlawful use of credit card, and uttering a forged instrument were three separate and distinct offenses. Buckley v. State, 1975, 322 N.E.2d 113, 163 Ind.App. 113.

Fraud was not lesser included offense of criminal conversion where fraud defined actions which went further than exerting unauthorized control over property of another, such as criminal conversion definition. McConnell v. State, 1982, 436 N.E.2d 1097.

In prosecution for fraud in use of credit card, evidence that credit or identification cards of people other than defendant and in name given to police by defendant as his identity were found in defendant's automobile when he was arrested was admissible to show intent, motive, purpose, identification and common scheme or plan. McConnell v. State, 1982, 436 N.E.2d 1097.

Defendant's convictions of theft under the Offenses Against Property Act, unlawful use of a credit card, and uttering a forged instrument were supported by sufficient evidence; the first offense was established by proof that defendant possessed another's credit card knowing it was not his own, exerted unauthorized control over it, and intended to deprive the other of its benefit; the second was established by proof that defendant, with intent to defraud store, obtained a tape deck by representing that he was the holder of the credit card without obtaining the owner's consent; and the third was established by proof that

defendant, with intent to defraud store, offered credit sales invoice knowing it to be forged. Buckley v. State, 1975, 322 N.E.2d 113, 163 Ind.App. 113.

Evidence including testimony that defendant presented credit card of another to retail store clerk and signed to credit instrument the name of person to whom credit card was made out but who, according to his testimony, had lost credit card and was not acquainted with defendant and did not authorize her to use card was sufficient to sustain conviction for fraud and forgery. Darnell v. State, 1972, 277 N.E.2d 366, 257 Ind. 613.

Where attempted credit card fraud is alleged, State need only prove that substantial step toward commission of crime occurred, along with requisite intent, but need not demonstrate act of forgery. Houston v. State, App. 3, Dist.1988, 528 N.E.2d 818.

Evidence was sufficient to sustain conviction of defendant for attempted credit card fraud; when asked how she intended to make payment for selection, defendant told salesperson that she was going to "put it on [her] charge," and then handed salesperson credit card belonging to victim, from which jury could reasonably determine that defendant made substantial step toward commission of fraud and would have completed crime but for unexpected interference of store personnel. Houston v. State, App. 3 Dist.1988, 528 N.E.2d 818.

IOWA CODE ANNOTATED

TITLE XVI. CRIMINAL LAW AND PROCEDURE
SUBTITLE 1. CRIME CONTROL AND CRIMINAL ACTS
CHAPTER 716A. COMPUTER CRIME

716A.1. Definitions

As used in this chapter, unless the context otherwise requires:

1. "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

2. "Computer" means an electronic device which performs logical, arithmetical, and memory functions by manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, computer software, and communication facilities which are connected or related to the computer in a computer system or computer network.

3. "Computer network" means a set of related, remotely connected devices and communication facilities including two or more computers with capability to transmit data among them through communication facilities.

4. "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

5. "Computer software" means a set of computer programs, procedures, or associated documentation used in the operation of a computer.

6. "Computer system" means related, connected or unconnected, computers or peripheral equipment.

7. "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, or is intended to be processed in a computer. Data may be in any form including, but not limited to, printouts, magnetic storage media, punched cards and as stored in the memory of a computer.

8. "Loss of property" means the greatest of the following:

   a. The retail value of the property involved.

   b. The reasonable replacement or repair cost, whichever is less.

9. "Loss of services" means the reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected.

10. "Property" means anything of value as defined in section 702.14, including but not limited to computers and computer data, information, software, and programs.

11. "Services" means the use of a computer, computer system, or computer network and includes, but is not limited to, computer time, data processing, and storage functions.

Title of Act:

An Act relating to the crimes of unauthorized access, computer damage, and computer theft and providing penalties. Acts 1984 (70 G.A.) ch. 1249.

716A.2. Unauthorized access

A person who knowingly and without authorization accesses a computer, computer system, or computer network commits a simple misdemeanor.

716A.3. Computer damage defined

A person commits computer damage when the person knowingly and without authorization damages or destroys a computer, computer system, computer network, computer software, computer program, or any other property as defined in section 716A.1, subsection 8, or knowingly and without authorization and with the intent to injure or defraud alters any computer, computer system, computer network, computer software, computer program, or any other property as defined in section 716A.1, subsection 8.

716A.4. Computer damage in the first degree

Computer damage is computer damage in the first degree when the damage results in a loss of property or services of more than ten thousand dollars. Computer damage in the first degree is a class "C" felony.

716A.5. Computer damage in the second degree

Computer damage is computer damage in the second degree when the damage results in a loss of property or services of more than one thousand dollars but not more than ten thousand dollars. Computer damage in the second degree is a class "D" felony.

716A.6. Computer damage in the third degree

Computer damage is computer damage in the third degree when the damage results in a loss of property or services of more than five hundred dollars but not more than one thousand dollars. Computer damage in the third degree is an aggravated misdemeanor.

716A.7. Computer damage in the fourth degree

Computer damage is computer damage in the fourth degree when the damage results in a loss of property or services of more than one hundred dollars but not more than five hundred dollars. Computer damage in the fourth degree is a serious misdemeanor.

716A.8. Computer damage in the fifth degree

Computer damage is computer damage in the fifth degree when the damage results in a loss of property or services of not more than one hundred dollars. Computer damage in the fifth degree is a simple misdemeanor.

716A.9. Computer theft defined

A person commits computer theft when the person knowingly and without authorization accesses or causes to be accessed a computer, computer system, or computer network, or any part thereof, for the purpose of obtaining services, information or property or knowingly and without authorization and with the intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of a computer, computer system, or computer network or any computer software or program, or data contained in a computer, computer system, or computer network.

716A.10. Computer theft in the first degree

Computer theft is computer theft in the first degree when the theft involves or results in a loss of services or property of more than ten thousand dollars. Computer theft in the first degree is a class "C" felony.

716A.11. Computer theft in the second degree

Computer theft is computer theft in the second degree when the theft involves or results in a loss of services or property of more than one thousand dollars but not more than ten thousand dollars. Computer theft in the second degree is a class "D" felony.

716A.12. Computer theft in the third degree

Computer theft is computer theft in the third degree when the theft involves or results in a loss of services or property of more than five hundred dollars but not more than one thousand dollars. Computer theft in the third degree is an aggravated misdemeanor.

716A.13. Computer theft in the fourth degree

Computer theft is computer theft in the fourth degree when the theft involves or results in a loss of services or property of more than one hundred dollars but not more than five hundred dollars.

Computer theft in the fourth degree is a serious misdemeanor.

716A.14. Computer theft in the fifth degree

Computer theft is computer theft in the fifth degree when the theft involves or results in a loss of services or property of not more than one hundred dollars. Computer theft in the fifth degree is a simple misdemeanor.

716A.15. Chapter not exclusive

This chapter does not preclude the applicability of any other provision of the law of this state which is not inconsistent with this chapter and which applies or may apply to an act or transaction in violation of this chapter.

716A.16. Printouts admissible as evidence

In a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary.

910.2. Restitution or community service to be ordered by sentencing court

In all criminal cases except simple misdemeanors under chapter 321, in which there is a plea of guilty, verdict of guilty, or special verdict upon which a judgment of conviction is rendered, the sentencing court shall order that restitution be made by each offender to the victims of the offender's criminal activities and, to the extent that the offender is reasonably able to pay, for crime victim assistance reimbursement, court costs, court-appointed attorney's fees or the expense of a public defender when applicable. However, victims shall be paid in full before restitution is paid for crime victim assistance reimbursement, court costs, court-appointed attorney's fees or for the expense of a public defender. In structuring a plan of restitution, the court shall . . .

KANSAS STATUTES ANNOTATED

CHAPTER 21. CRIMES AND PUNISHMENTS
KANSAS CRIMINAL CODE (ARTICLES 31 TO 46)
PART II. PROHIBITED CONDUCT
ARTICLE 37. CRIMES AGAINST PROPERTY

21-3755. Computer crime; unlawful computer access.

(1) As used in this section, the following words and phrases shall have the meanings respectively ascribed thereto:

(a) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network.

(b) "Computer" means an electronic device which performs work using programmed instruction and which has one or more of the capabilities of storage, logic, arithmetic or communication and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

(c) "Computer network" means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(d) "Computer program" means a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(e) "Computer software" means computer programs, procedures and associated documentation concerned with the operation of a computer system.

(f) "Computer system" means a set of related computer equipment or devices and computer software which may be connected or unconnected.

(g) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card or marketable security.

(h) "Property" includes, but is not limited to, financial instruments, information, electronically produced or stored data, supporting documentation and computer software in either machine or human readable form and any other tangible or intangible item of value.

(i) "Services" includes, but is not limited to, computer time, data processing and storage functions and other uses of a computer, computer system or computer network to perform useful work.

(j) "Supporting documentation" includes, but is not limited to, all documentation

used in the construction, classification, implementation, use or modification of computer software, computer programs or data.

(2) Computer crime is:

(a) Willfully and without authorization gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property;

(b) using a computer, computer system, computer network or any other property for the purpose of devising or executing a scheme or artifice with the intent to defraud or for the purpose of obtaining money, property, services or any other thing of value by means of false or fraudulent pretense or representation; or

(c) willfully exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property.

Computer crime which causes a loss of the value of less than $150 is a class A misdemeanor.

Computer crime which causes a loss of the value of $150 or more is a class E felony.

(3) In any prosecution for computer crime, it is a defense that the property or services were appropriated openly and avowedly under a claim of title made in good faith.

(4) Unlawful computer access is willfully, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network or to any computer software, program, documentation, data or property contained in any computer, computer system or computer network.

Unlawful computer access is a class A misdemeanor.

(5) This section shall be part of and supplemental to the Kansas criminal code.

KENTUCKY REVISED STATUTES ANNOTATED

TITLE XL. CRIMES AND PUNISHMENTS
CHAPTER 434. OFFENSES AGAINST PROPERTY BY FRAUD
UNLAWFUL ACCESS TO A COMPUTER

§434.840 Definitions.

For the purposes of KRS 434.845 and 434.850, the following words (including any form of the word) and terms shall have the following meanings:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

(2) "Computer" means a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job;

(3) "Computer network" means a set of two or more computer systems that transmit data over communication circuits connecting them;

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data;

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network;

(6) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(7) "Data" is a representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be stored or processed, or is being stored or processed, or has been stored or processed, in a computer, computer system or computer network;

(8) "Financial instruments" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, or marketable security, or any computer system representation thereof;

(9) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(10) "To process" is to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(11) "Property" includes, but is not limited to, intellectual property, financial instruments,

data, computer programs, documentation associated with data, computers, computer systems and computer programs, all in machine-readable or human-readable form, and any tangible or intangible item of value; and

(12) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer program, or data to perform tasks.

§434.845 Unlawful access to a computer in the first degree.

(1) A person is guilty of unlawful access to a computer in the first degree when he knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of:

(a) Devising or executing any scheme or artifice to defraud; or

(b) Obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises; or

(c) Altering, damaging, destroying, or attempting to alter, damage, or destroy, any computer, computer system, or computer network, or any computer software, program, or data.

(2) Accessing, attempting to access, or causing to be accessed any computer software, computer program, data, computer, computer system, computer network, or any part thereof, even though fraud, false or fraudulent pretenses, representations, or promises may have been involved in the access or attempt to access shall not constitute a violation of this section if the sole purpose of the access was to obtain information and not to commit any other act proscribed by this section.

(3) Unlawful access to a computer in the first degree is a Class C felony.

§434.850 Unlawful access to computer in the second degree.

(1) A person is guilty of unlawful access to a computer in the second degree when he without authorization knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof.

(2) Unlawful access to a computer in the second degree is a Class A misdemeanor.

§434.855 Misuse of computer information.

(1) A person is guilty of misuse of computer information when he:

(a) Receives, conceals, or uses, or aids another in doing so, any proceeds of a violation of KRS 434.845; or

(b) Receives, conceals, or uses or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing the same to have been used in or obtained from a violation of KRS 434.845.

(2) Misuse of computer information is a Class C felony.

§434.860 Venue.

For the purpose of venue under the provisions of KRS 434.845, 434.850 or 434.855, any violation of KRS 434.845, 434.850 or 434.855 shall be considered to have been committed: in any county in which any act was performed in furtherance of any transaction violating KRS 434.845, 434.850 or 434.855; in any county in which any violator had control or possession of any proceeds of said violation or of any books, records, documents, property, financial instrument, computer software, computer program or other material, objects or items which were used in furtherance of said violation; and in any county from which, to which or through which any access to a computer, computer system, or computer network was made whether by wires, electromagnetic waves, microwaves or any other means of communication.

KENTUCKY REVISED STATUTES ANNOTATED

TITLE L. KENTUCKY PENAL CODE
CHAPTER 514. THEFT AND RELATED OFFENSES

§514.030 Theft by unlawful taking or disposition.

(1) A person is guilty of theft by unlawful taking or disposition when he unlawfully:

(a) Takes or exercises control over movable property of another with intent to deprive him thereof; or

(b) Obtains immovable property of another or any interest therein with intent to benefit himself or another not entitled thereto.

(2) Theft by unlawful taking or disposition is a Class A misdemeanor unless the value of the property is three hundred dollars ($300) or more, in which case it is a Class D felony.

LOUISIANA STATUTES ANNOTATED

LOUISIANA REVISED STATUTES
TITLE 14. CRIMINAL LAW
CHAPTER 1. CRIMINAL CODE
PART III. OFFENSES AGAINST PROPERTY
SUBPART D. COMPUTER RELATED CRIME

§73.1. Definitions

As used in this Subpart unless the context clearly indicates otherwise:

(1) "Access" means to program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources, including data or programs, of a computer, computer system, or computer network.

(2) "Computer" includes an electronic, magnetic, optical, or other high-speed data processing device or system performing logical, arithmetic, and storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system. "Computer" shall not include an automated typewriter or typesetter, a machine designed solely for word processing, or a portable hand-held calculator, nor shall "computer" include any other device which might contain components similar to those in computers but in which the components have the sole function of controlling the device for the single purpose for which the device is intended.

(3) "Computer network" means a set of related, remotely connected devices and communication facilities including at least one computer system with capability to transmit data through communication facilities.

(4) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(5) "Computer services" means providing access to or service or data from a computer, a computer system, or a computer network.

(6) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with operation of a computer system.

(7) "Computer system" means a set of functionally related, connected or unconnected, computer equipment, devices, or computer software.

(8) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, access card as defined in R.S. 14:67.3, or marketable security.

(9) "Intellectual property" includes data, computer programs, computer software, trade secrets as defined in R.S. 51:1431(4), copyrighted materials, and confidential or proprietary information, in any form or medium, when such is stored in, produced by, or intended for use or storage with or in a computer, a computer system, or a computer network.

(10) "Proper means" include:

(a) Discovery by independent invention;

(b) Discovery by "reverse engineering", that is by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must be by lawful means;

(c) Discovery under license or authority of the owner;

(d) Observation of the property in public use or on public display; or

(e) Discovery in published literature.

(11) "Property" means property as defined in R.S. 14:2(8) and shall specifically include but not be limited to financial instruments, electronically stored or produced data, and computer programs, whether in machine readable or human readable form.

Title of Act:

An Act to enact Subpart D of Part III of Chapter 1 of Title 14 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 14:73.1 through R.S. 14:73.5, relative to computer related crimes, to provide certain definitions and penalties for offenses against intellectual property, against computer equipment and supplies, against certain computer users, and for computer fraud, and otherwise to provide with respect thereto. Acts 1984, No. 711.

SELECTED LEGISLATIVE HISTORY

Definition of "computer" in subsec. 2 of this section was readily understandable by ordinary persons of reasonable intelligence, and was not unconstitutionally vague. State v. Azar, Sup.1989, 539 So.2d 1222, certiorari denied 110 S.Ct. 82, 493 U.S. 823, 107 L.Ed.2d 48.

Subsection 1 in this section was not rendered unconstitutionally vague under Const. Art. 1, § 13 by failure to define "access" as "knowing access," since required criminal intent was intent to defraud, and not intent to access. State v. Azar, Sup.1989, 539 So.2d 1222, certiorari denied 110 S.Ct. 82, 493 U.S. 823, 107 L.Ed.2d 48.

"Intellectual property," for purposes of this section, is defined as data, computer programs, computer software, trade secrets, copyrighted materials, and confidential or proprietary information, in any form or medium, when such is stored in, produced by, or intended for use or storage with or in a computer, computer system, or computer network. State v. Tanner, App. 5 Cir.1988, 534 So.2d 535.

§73.2. Offenses against intellectual property

A. An offense against intellectual property is the intentional:

(1) Destruction, insertion, or modification, without consent, of intellectual property; or

(2) Disclosure, use, copying, taking, or accessing, without consent, of intellectual property.

B. (1) Whoever commits an offense against intellectual property shall be fined not more than five hundred dollars, or imprisoned for not more than six months, or both, for commission of the offense.

(2) However, when the damage or loss amounts to a value of five hundred dollars or more, the offender may be fined not more than ten thousand dollars, or imprisoned with or without hard labor, for not more than five years, or both.

C. The provisions of this Section shall not apply to disclosure, use, copying, taking, or accessing by proper means as defined in this Subpart.

SELECTED LEGISLATIVE HISTORY

Evidence was sufficient to sustain defendant's conviction of offense against intellectual property for copying copyrighted software program of former employer and putting it to use in his own business. State v. Tanner, App. 5 Cir.1988, 534 So.2d 535.

§73.3. Offenses against computer equipment or supplies

A. An offense against computer equipment or supplies is the intentional modification or destruction, without consent, of computer equipment or supplies used or intended to be used in a computer, computer system, or computer network.

B. (1) Whoever commits an offense against computer equipment or supplies shall be fined not more than five hundred dollars, or be imprisoned for not more than six months, or both.

(2) However, when the damage or loss amounts to a value of five hundred dollars or more, the offender may be fined not more than ten thousand dollars, or imprisoned with or without hard labor, for not more than five years, or both.

§73.4. Offenses against computer users

A. An offense against computer users is the intentional denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network, or computer services.

B. (1) Whoever commits an offense against computer users shall be fined not more than five hundred dollars, or be imprisoned for not more than six months, or both, for commission of the offense.

(2) However, when the damage or loss amounts to a value of five hundred dollars or more, the offender may be fined not more than ten thousand dollars ...

MAINE REVISED STATUTES ANNOTATED

TITLE 17-A. MAINE CRIMINAL CODE
PART 2. SUBSTANTIVE OFFENSES
CHAPTER 18. COMPUTER CRIMES

§431. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. "Access" means to gain logical entry into, instruct, communicate with, store data in or retrieve data from any computer resource.

2. "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

3. "Computer information" means a representation of information, knowledge, facts, concepts or instructions that are confidential or proprietary, are being prepared or have been prepared from an organized set of data and are located in computer memory or on magnetic, optical or mechanical media transferable directly to or useable directly by a computer as a source of data or instructions.

4. "Computer network" means a combination of one or more computers and communication facilities with the capability to transmit information among the devices or computers.

5. "Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, cause the computer to process data.

6. "Computer software" means a set of computer programs, procedures and associated documentation used in the operation of a computer system.

7. "Computer system" means any combination of a computer or computers with the documentation, computer software or physical facilities supporting the computer.

8. "Computer resource" means a computer program, computer software, computer system, computer network, computer information or any combination thereof.

9. "Computer virus" means any computer instruction, information, data or program that degrades the performance of a computer resource; disables, damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer program, data or instruction is executed or when some other event takes place in the host computer resource, data or instruction.

10. "Damage" means to destroy, alter, disrupt, delete, add, modify, or rearrange any computer resource by any means.

11. "Not authorized" and "unauthorized" mean not having consent or permission of the

owner, or person licensed or authorized by the owner to grant consent or permission, to access or use any computer resource, or accessing or using any computer resource in a manner exceeding the consent or permission.

§432. Criminal invasion of computer privacy

1. A person is guilty of criminal invasion of computer privacy if the person intentionally accesses any computer resource knowing that the person is not authorized to do so.

2. Criminal invasion of computer privacy is a Class D crime.

§433. Aggravated criminal invasion of computer privacy

1. A person is guilty of aggravated criminal invasion of computer privacy if the person:

   A. Intentionally makes an unauthorized copy of any computer program, computer software or computer information, knowing that the person is not authorized to do so;

   B. Intentionally or knowingly damages any computer resource of another person, having no reasonable ground to believe that the person has the right to do so; or

   C. Intentionally or knowingly introduces or allows the introduction of a computer virus into any computer resource, having no reasonable ground to believe that the person has the right to do so.

2. Aggravated criminal invasion of computer privacy is a Class C crime.

ANNOTATED CODE OF MARYLAND

ARTICLE 27. CRIMES AND PUNISHMENTS.
I. CRIMES AND PUNISHMENTS
CREDIT CARD OFFENSES

§146 Unauthorized access to computers prohibited.

(a) Definitions. -- In this section the following words have the meanings indicated.

(1) (i) "Computer" means an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions.

(ii) "Computer" includes any property, data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.

(iii) "Computer" does not include an automated typewriter or typesetter, or a portable calculator.

(2) "Computer control language" means any ordered statements that direct a computer to perform specific functions.

(3) "Computer data base" means a representation of information, knowledge, facts, concepts, or instructions that:

(i) Are being prepared or have been prepared in a formalized manner or are or have been produced by a computer, computer system, or computer network; and

(ii) Are intended for use in a computer, computer system, or computer network.

(4) "Computer network" means the interconnection of 1 or more computers through:

(i) The use of satellite, microwave, line, or other communication media; and

(ii) Terminals or a complex consisting of 2 or more interconnected computers whether or not the interconnection is continuously maintained.

(5) "Computer program" means an ordered set of instructions or statements that may interact with related data that, when executed in a computer system, causes the computer to perform specified functions.

(6) "Computer services" includes, but is not limited to, computer time, data processing, and storage functions.

(7) "Computer software" means computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.

(8) "Computer system" means 1 or more connected or unconnected computers, peripheral devices, software, data, or programs.

(9) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.

(b) Other applicable Code provisions. -- This section does not preclude the applicability of any other provision of this Code.

(c) Illegal access.

(1) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services.

(2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to:

(i) Cause the malfunction or interrupt the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services; or

(ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer data base, or any part of these systems or services.

(3) A person may not intentionally, willfully, and without authorization:

(i) Identify or attempt to identify any valid access codes; or

(ii) Distribute or publicize any valid access codes to any unauthorized person.

(d) Penalty.

(1) Any person who violates any provision of subsection (c) (1) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding $1,000 or imprisonment not exceeding 3 years or both.

(2) Any person who violates any provision of subsection (c) (2) or (c) (3) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding $5,000 or imprisonment not exceeding 5 years or both.

(e) Scope of offenses; jurisdiction.

(1) When illegal access to a computer, computer network, computer control language, computer system, computer services, computer software, computer data base, or any part of these systems or services is committed in violation of this section pursuant to 1 scheme or continuing course of conduct, the conduct may be considered as 1 offense.

(2) A court of competent jurisdiction in this State may try a person who allegedly violates any provision of subsection (c) of this section in any county in this State where:

(i) The person performs the act; or

(ii) The accessed computer is located.

MICHIGAN COMPILED LAWS ANNOTATED

CHAPTER 752. CRIMES AND OFFENSES
FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND COMPUTER NETWORKS

752.791. Meanings of words and phrases

Sec. 1. For the purposes of this act, the words and phrases defined in sections 2 and 3 [FN1] have the meanings ascribed to them in those sections.

[FN1] Sections 752.792 and 752.793.

752.792. Definitions

Sec. 2.

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise use the resources of, a computer, computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes input, output, processing, storage, software, or communication facilities which are connected or related to a device in a system or network.

(3) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of 2 or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

752.793. Definitions

Sec. 3.

(1) "Property" includes financial instruments; information, including electronically produced data; computer software and programs in either machine or human readable form; and any other tangible or intangible item of value.

(2) "Services" includes computer time, data processing, and storage functions.

752.794. Access to computers for devising or executing scheme to defraud or obtain money, property, or service

Sec. 4. A person shall not, for the purpose of devising or executing a scheme or artifice with intent to defraud or for the purpose of obtaining money, property, or a service by means of a false or fraudulent pretense, representation, or promise with intent to, gain access to or cause access to be made to a computer, computer system, or computer network.

SELECTED LEGISLATIVE HISTORY

Computer fraud convictions of Department of Social Services employee were not supported by sufficient evidence; evidence established that employee completed documentation containing fraudulent information and submitted it to her supervisor in usual course of business and under standard procedure, and relevant statute requires more than merely supplying information which ultimately finds its way into computer system in normal course of business. People v. Jemison (1991) 466 N.W.2d 378,

752.795. Gaining access to alter, damage, or destroy computers, computer programs, or data

Sec. 5. A person shall not intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computer network.

752.796. Use of computers to commit violations of certain sections

Sec. 6. A person shall not utilize a computer, computer system, or computer network to commit a violation of section 174 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.174 of the Michigan Compiled Laws, section 279 of Act No. 328 of the Public Acts of 1931, being section 750.279 of the Michigan Compiled Laws, section 356 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.356 of the Michigan Compiled Laws, or section 362 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.362 of the Michigan Compiled Laws.

752.797. Violations; misdemeanor, felony, penalties

Sec. 7. A person who violates this act, if the violation involves $100.00 or less, is guilty of a misdemeanor. If the violation involves more than $100.00, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than $5,000.00, or both.

609.87. Computer crime; definitions

Subd 1. Applicability.
For purposes of sections 609.87 to 609.89, and section 609.891, the terms defined in this section have the meanings given them.

Subd. 2. Access.
"Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

Subd. 3. Computer.
"Computer" means an electronic device which performs logical, arithmetic or memory functions by the manipulations of signals, including but not limited to electronic or magnetic impulses.

Subd. 4. Computer system.
"Computer system" means related, connected or unconnected, computers and peripheral equipment.

Subd. 5. Computer network.
"Computer network" means the interconnection of a communication system with a computer through a remote terminal, or with two or more interconnected computers or computer systems, and includes private and public telecommunications networks.

Subd. 6. Property.
"Property" includes, but is not limited to, electronically processed or produced data and information contained in a computer or computer software in either machine or human readable form.

Subd. 7. Services.
"Services" includes but is not limited to, computer time, data processing, and storage functions.

Subd. 8. Computer program.
"Computer program" means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which directs the functioning of a computer system in a manner designed to provide appropriate products from the computer.

Subd. 9. Computer software.
"Computer software" means a computer program or procedures, or associated documentation concerned with the operation of a computer.

Subd. 10. Loss.
"Loss" means the greatest of the following:

(a) the retail market value of the property or services involved;

(b) the reasonable repair or replacement cost, whichever is less; or

(c) the reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected.

Subd. 11. Computer security system.

"Computer security system" means a software program or computer device that:

(1) is intended to protect the confidentiality and secrecy of data and information stored in or accessible through the computer system; and

(2) displays a conspicuous warning to a user that the user is entering a secure system or requires a person seeking access to knowingly respond by use of an authorized code to the program or device in order to gain access.

Subd. 12. Destructive computer program.

"Destructive computer program" means a computer program that performs a destructive function or produces a destructive product. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program; disables the computer, associated peripherals or a computer program; or destroys or alters computer programs or data. A program produces a destructive product if it produces unauthorized data, including data that make computer memory space unavailable; results in the unauthorized alteration of data or computer programs; or produces a destructive computer program, including a self-replicating computer program.

609.891. Unauthorized computer access

Subd 1. Crime.

A person is guilty of unauthorized computer access if the person intentionally and without authority attempts to or does penetrate a computer security system.

Subd. 2. Felony.

(a) A person who violates subdivision 1 in a manner that creates a grave risk of causing the death of a person is guilty of a felony and may be sentenced to a term of imprisonment of not more than ten years or to payment of a fine of not more than $20,000, or both.

(b) A person who is convicted of a second or subsequent gross misdemeanor violation of subdivision 1 is guilty of a felony and may be sentenced under paragraph (a).

Subd. 3. Gross misdemeanor.

(a) A person who violates subdivision 1 in a manner that creates a risk to public health and safety is guilty of a gross misdemeanor and may be sentenced to imprisonment for a term of not more than one year or to payment of a fine of not more than $3,000, or both.

(b) A person who violates subdivision 1 in a manner that compromises the security of data that are protected under section 609.52, subdivision 2, clause (8), or are not public data as defined in section 13.02, subdivision 8a, is guilty of a gross misdemeanor and may be sentenced under paragraph (a).

(c) A person who is convicted of a second or subsequent misdemeanor violation of subdivision 1 within five years is guilty of a gross misdemeanor and may be sentenced under paragraph (a).

Subd. 4. Misdemeanor. A person who violates subdivision 1 is guilty of a misdemeanor and may be sentenced to imprisonment for a term of not more than 90 days or to payment of a fine of not more than $700, or both.

MISSISSIPPI CODE 1972 ANNOTATED

TITLE 97. CRIMES

CHAPTER 19. FALSE PRETENSES AND CHEATS

§97-19-9. Credit cards--definitions.

The following words and phrases as used in sections 97-19-5 through 97-19-29 shall have the following meanings ascribed to them, unless a different meaning is plainly required by the context:

(a) "Cardholder" is defined as the person or organization named on the face of a credit card, as defined hereinafter, to whom or for whose benefit the credit card is issued by an issuer.

(b) "Credit card" is defined as any instrument or device, whether known as a credit card, credit plate or by any other name, issued with or without fee by an issuer for the use of the cardholder or one authorized by him in obtaining money, goods, property, services or anything else of value on credit or in consideration of an undertaking or guaranty of the issuer of the payment of a check or draft drawn by the cardholder or one authorized by him, and shall include a card issued by a financial institution to be used in operating an automatic unmanned cash dispensing machine.

(c) "Expired credit card" means a credit card which is no longer valid because the term shown on its face has elapsed.

(d) "Issuer" is defined as any business organization or financial institution, including but not limited to merchants, state and national banks, and any and all other persons, firms, corporations, trusts, and organizations, or any duly authorized agent thereof, which issues a credit card.

(e) "Receives" or "receiving" is defined as acquiring possession of or control of or accepting as security for a loan a credit card.

(f) "Revoked credit card" is defined as a credit card which is no longer valid because permission to use it has been suspended or terminated by the issuer.

(g) A credit card is "incomplete" if part of the matter other than the signature of the cardholder which an issuer requires to appear on the credit card before it can be used by a cardholder has not been stamped, embossed, imprinted or written on said card.

(h) A person "falsely makes" a credit card when he makes or draws in whole or in part a device or instrument which purports to be the credit card of a named issuer, but which is not in fact such a credit card because the issuer did not authorize the making or drawing of said card; or when one materially alters a credit card which was validly issued.

(i) A person "falsely embosses" a credit card when, without the authorization of the named issuer, he completes a credit card by adding any other matter than the signature of the cardholder which an issuer requires to appear on the credit card before it can be used by a cardholder.

MISSISSIPPI CODE 1972 ANNOTATED

TITLE 97. CRIMES

CHAPTER 45. COMPUTER CRIMES

§97-45-1. Definitions.

For the purposes of this chapter, the following words shall have the meanings ascribed herein unless the context clearly requires otherwise:

(a) "Access" means to program, to execute programs on, to communicate with, store data in, retrieve data from or otherwise make use of any resources, including data or programs, of a computer, computer system or computer network.

(b) "Computer" includes an electronic, magnetic, optical or other high-speed data processing device or system performing logical arithmetic and storage functions and includes any property, data storage facility or communications facility directly related to or operating in conjunction with such device or system. "Computer" shall not include an automated typewriter or typesetter, a machine designed solely for word processing which contains no data base intelligence or a portable hand-held calculator nor shall "computer" include any other device which contains components similar to those in computers but in which the components have the sole function of controlling the device for the single purpose for which the device is intended unless the thus controlled device is a processor of data or is a storage of intelligence in which case it too is included.

(c) "Computer network" means a set of related, remotely connected devices and communication facilities including at least one (1) computer system with the capability to transmit data through communication facilities.

(d) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(e) "Computer software" means a set of computer programs, procedures and associated documentation concerned with operation of a computer system.

(f) "Computer system" means a set of functionally related, connected or unconnected, computer equipment, devices or computer software.

(g) "Computer services" means providing access to or service or data from a computer, a computer system or a computer network and includes the actual data processing.

(h) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card as defined in Section 97-19-9(b), Mississippi Code of 1972, or

marketable security.

(i) "Intellectual property" includes data, computer programs, computer software, trade secrets, copyrighted materials and confidential or proprietary information in any form or medium when such is stored in, produced by or intended for use or storage with or in a computer, a computer system or a computer network.

(j) "Property" means property as defined in Section 1-3-45, Mississippi Code of 1972, and shall specifically include, but not be limited to, financial instruments, electronically stored or produced data and computer programs, whether in machine readable or human readable form.

(k) "Proper means" includes:

(i) Discovery by independent invention;

(ii) Discovery by "reverse engineering"; that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must be by lawful means;

(iii) Discovery under license or authority of the owner;

(iv) Observation of the property in public use or on public display; or

(v) Discovery in published literature.

(l) "Use" means to make use of, to convert to one's service, to avail oneself of or to employ. In the context of this act, "use" includes to instruct, communicate with, store data in or retrieve data from, or otherwise utilize the logical arithmetic or memory functions of a computer.

§97-45-3. Computer fraud; penalties.

(1) Computer fraud is the accessing or causing to be accessed of any computer, computer system, computer network, or any part thereof with the intent to:

(a) Defraud; or

(b) Obtain money, property or services by means of false or fraudulent conduct, practices or

representations; or through the false or fraudulent alteration, deletion or insertion of programs or data.

(2) Whoever commits the offense of computer fraud shall be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00), or by imprisonment for not more than five (5) years, or by both such fine and imprisonment.

NOTES

Computer programs as property subject to theft. 18 ALR3d 1121.
Criminal liability for misappropriation of trade secret. 84 ALR3d 967.
Disclosure or use of computer application software as misappropriation of trade secret. 30 ALR4th 1250.

Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems. 51 ALR4th 971.

What is computer "trade secret" under state law. 53 ALR4th 1046.

§97-45-5. Offense against computer users; penalties.

(1) An offense against computer users is the intentional:

(a) Denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network or computer services; or

(b) Use or disclosure to another, without consent, of the numbers, codes, passwords or other means of access to a computer, a computer system, a computer network or computer services.

(2) Whoever commits an offense against computer users shall be punished, upon conviction, by a fine of not more than One Thousand Dollars ($1,000.00), or by imprisonment for not more than six (6) months, or by both such fine and imprisonment. However, when the damage or loss amounts to a value of One Hundred Dollars ($100.00) or more, the offender may be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00), or imprisonment for

not more than five (5) years, or by both such fine and imprisonment.

§97-45-7. Offense against computer equipment; penalties.

(1) An offense against computer equipment or supplies is the intentional modification or destruction, without consent, of computer equipment or supplies used or intended to be used in a computer, computer system or computer network.

(2) Whoever commits an offense against computer equipment or supplies shall be punished, upon conviction, by a fine of not more than One Thousand Dollars ($1,000.00), or by imprisonment for not more than six months or both such fine and imprisonment. However, when the damage or loss amounts to a value of One Hundred Dollars ($100.00) or more, the offender may be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00) or by imprisonment for not more than five (5) years, or by both such fine and imprisonment.

§97-45-9. Offense against intellectual property; penalties.

(1) An offense against intellectual property is the intentional:

(a) Destruction, insertion or modification, without consent, of intellectual property; or

(b) Disclosure, use, copying, taking or accessing, without consent, of intellectual property.

(2) Whoever commits an offense against intellectual property shall be punished, upon conviction, by a fine of not more than One Thousand Dollars ($1,000.00), or by imprisonment for not more than six (6) months, or by both such fine and imprisonment. However, when the damage or loss amounts to a value of One Hundred Dollars ($100.00) or more, the offender may be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00) or by imprisonment for not more than five (5) years, or by both such fine and imprisonment.

(3) The provisions of this section shall not apply to the disclosure, use, copying, taking, or accessing by proper means as defined in this chapter.

§97-45-11. Venue.

For the purposes of venue under the provisions of this chapter, any violation of this chapter shall be considered to have been committed:

(a) In any county in which any act was performed in furtherance of any transaction violating this chapter; and

(b) In any county from which, to which or through which any access to a computer, computer system or computer network was made, whether by wire, electromagnetic waves, microwaves or any other means of communication.

§97-45-13. Effect on other offenses.

The criminal offenses created by this chapter shall not be deemed to supersede, or repeal, any other criminal offense.

569.095. Tampering with computer data, penalties

1. A person commits the crime of tampering with computer data if he knowingly and without authorization or without reasonable grounds to believe that he has such authorization:

   (1) Modifies or destroys data or programs residing or existing internal to a computer, computer system, or computer network; or

   (2) Modifies or destroys data or programs or supporting documentation residing or existing external to a computer, computer system, or computer network; or

   (3) Discloses or takes data, programs, or supporting documentation, residing or existing internal or external to a computer, computer system, or computer network; or

   (4) Discloses or takes a password, identifying code, personal identification number, or other confidential information about a computer system or network that is intended to or does control access to the computer system or network;

   (5) Accesses a computer, a computer system, or a computer network, and intentionally examines information about another person;

   (6) Receives, retains, uses, or discloses any data he knows or believes was obtained in violation of this subsection.

2. Tampering with computer data is a class A misdemeanor, unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, the value of which is one hundred fifty dollars or more, in which case tampering with computer data is a class D felony.

569.097. Tampering with computer equipment, penalties

1. A person commits the crime of tampering with computer equipment if he knowingly and without authorization or without reasonable grounds to believe that he has such authorization:

(1) Modifies, destroys, damages, or takes equipment or data storage devices used or intended to be used in a computer, computer system, or computer network; or

(2) Modifies, destroys, damages, or takes any computer, computer system, or computer network.

2. Tampering with computer equipment is a class A misdemeanor, unless:

(1) The offense is committed for the purpose of executing any scheme or artifice to defraud or obtain any property, the value of which is one hundred fifty dollars or more, in which case it is a class D felony; or

(2) The damage to such computer equipment or to the computer, computer system, or computer network is one hundred fifty dollars or more but less than one thousand dollars, in which case it is a class D felony; or

(3) The damage to such computer equipment or to the computer, computer system, or computer network is one thousand dollars or greater, in which case it is a class C felony.

569.099. Tampering with computer users, penalties

1. A person commits the crime of tampering with computer users if he knowingly and without authorization or without reasonable grounds to believe that he has such authorization:

(1) Accesses or causes to be accessed any computer, computer system, or computer network; or

(2) Denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, or on behalf of, or in conjunction with another.

2. The offense of tampering with computer users is a class A misdemeanor unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, the value of which is one hundred fifty dollars or more, in which case tampering with computer users is a class D felony.

MONTANA CODE ANNOTATED

TITLE 45. CRIMES
CHAPTER 1. GENERAL PRELIMINARY PROVISIONS
PART 2. CLASSIFICATION AND LIMITATIONS

45-1-205. General time limitations.

(1) (a) A prosecution for deliberate, mitigated, or negligent homicide may be commenced at any time.

(b) A prosecution under 45-5-502 through 45-5-505, 45-5-507, or 45-5-625 may be commenced within 5 years after the victim reaches the age of 18 if the victim was less than 18 years old at the time the offense occurred.

(2) Except as otherwise provided by law, prosecutions for other offenses are subject to the following periods of limitation:

(a) A prosecution for a felony must be commenced within 5 years after it is committed.

(b) A prosecution for a misdemeanor must be commenced within 1 year after it is committed.

(3) The period prescribed in subsection (2) is extended in a prosecution for theft involving a breach of fiduciary obligation to an aggrieved person as follows:

(a) if the aggrieved person is a minor or incompetent, during the minority or incompetency or within 1 year after the termination thereof;

(b) in any other instance, within 1 year after the discovery of the offense by the aggrieved person or by a person who has legal capacity to represent an aggrieved person or has a legal duty to report the offense and is not himself a party to the offense or, in the absence of such discovery, within 1 year after the prosecuting officer becomes aware of the offense.

(4) The period prescribed in subsection (2) shall be extended in a prosecution for unlawful use of a computer, and prosecution shall be brought within 1 year after the discovery of the offense by the aggrieved person or by a person who has legal capacity to represent an aggrieved person or has a legal duty to report the offense and is not himself a party to the offense or, in the absence of such discovery, within 1 year after the prosecuting officer becomes aware of the offense.

(5) The period prescribed in subsection (2) is extended in a prosecution for misdemeanor fish and wildlife violations under Title 87, and prosecution must be brought within 3 years after an offense

is committed.

(6) An offense is committed either when every element occurs or, when the offense is based upon a continuing course of conduct, at the time when the course of conduct is terminated. Time starts to run on the day after the offense is committed.

(7) A prosecution is commenced either when an indictment is found or an information or complaint is filed.

MONTANA CODE ANNOTATED

TITLE 45. CRIMES
CHAPTER 6. OFFENSES AGAINST PROPERTY
PART 3. THEFT AND RELATED OFFENSES

45-6-311. Unlawful use of a computer.

(1) A person commits the offense of unlawful use of a computer if he knowingly or purposely:

(a) obtains the use of any computer, computer system, or computer network without consent of the owner;

(b) alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or

(c) obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

(2) A person convicted of the offense of unlawful use of a computer involving property not exceeding $300 in value shall be fined not to exceed $500 or be imprisoned in the county jail for a term not to exceed 6 months, or both. A person convicted of the offense of unlawful use of a computer involving property exceeding $300 in value shall be fined not more than 2 1/2 times the value of the property used, altered, destroyed, or obtained or be imprisoned in the state prison for a term not to exceed 10 years, or both.

NEBRASKA REVISED STATUTES OF 1943

CHAPTER 28. CRIMES AND PUNISHMENTS
ARTICLE 13. MISCELLANEOUS OFFENSES
(P) COMPUTERS

§28-1341. Act, how cited.

Sections 28-1341 to 28-1348 shall be known and may be cited as the Computer Crimes Act.

§28-1342. Legislative findings and declarations.

The Legislature finds and declares that our society is increasingly dependent on computers, that important personal, financial, medical, and historical data is stored in computers, and that valuable data stored can be lost due to criminal action.

The Legislature further finds that specific criminal statutes are necessary to cover the actions of persons who intentionally destroy data or commit fraud using computers.

§28-1343. Terms, defined.

For purposes of the Computer Crimes Act:

(1) Access shall mean to instruct, communicate with, store data in, retrieve data from, or otherwise use the resources of a computer, computer system, or computer network;

(2) Computer shall mean a high-speed data processing device or system which performs logical, arithmetic, data storage and retrieval, communication, memory, or control functions by the manipulation of signals, including, but not limited to, electronic or magnetic impulses, and shall include any input, output, data storage, processing, or communication facilities directly related to or operating in conjunction with any such device or system;

(3) Computer network shall mean the interconnection of a communications system with a computer through a remote terminal or with two or more interconnected computers or computer systems;

(4) Computer program shall mean an instruction or statement or a series of instructions or statements in a form acceptable to a computer which directs the functioning of a computer system in a manner designed to provide appropriate products from the computer;

(5) Computer security system shall mean a computer program or device that:

(a) Is intended to protect the confidentiality and secrecy of data and information stored in or accessible through the computer system; and

(b) Displays a conspicuous warning to a user that the user is entering a secure system or requires a person seeking access to knowingly respond by use of an authorized code to the program or device in order to gain access;

(6) Computer software shall mean a computer program of procedures or associated documentation concerned with the operation of a computer;

(7) Computer system shall mean related computers and peripheral equipment, whether connected or unconnected;

(8) Data shall mean a representation of information, facts, knowledge, concepts, or instructions prepared in a formalized or other manner and intended for use in a computer or computer network;

(9) Destructive computer program shall mean a computer program that performs a destructive function or produces a destructive product;

(10) Destructive function shall mean a function that

(a) degrades the performance of a computer, its associated peripheral equipment, or a computer program,

(b) disables a computer, its associated peripheral equipment, or a computer program, or

(c) alters a computer program or data;

(11) Destructive product shall mean a product that:

(a) Produces unauthorized data, including data that make computer memory space unavailable;

(b) results in the unauthorized alteration of data or a computer program; or

(c) produces a destructive computer program, including, but not limited to, a self-replicating

program;

(12) Loss shall mean the greatest of the following:

(a) The retail market value of the property or services involved;

(b) The reasonable repair or replacement cost whichever is less; or

(c) The reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected;

(13) Property shall include, but not be limited to, electronically processed or electronically produced data and information in computer software whether in human or computer readable form; and

(14) Services shall include, but not be limited to, computer time, data processing, and storage functions.

§28-1343.01. Unauthorized computer access; penalty.

(1) A person commits the offense of unauthorized computer access if the person intentionally and without authority penetrates a computer security system.

(2) A person who violates subsection (1) of this section in a manner that creates a grave risk of causing the death of a person shall be guilty of a Class IV felony.

(3) A person who violates subsection (1) of this section in a manner that creates a risk to public health and safety shall be guilty of a Class I misdemeanor.

(4) A person who violates subsection (1) of this section in a manner that compromises the security of data shall be guilty of a Class II misdemeanor.

§28-1344. Unlawful acts; depriving or obtaining property or services; penalties.

Any person who intentionally accesses or causes to be accessed, directly or indirectly, any computer, computer system, computer software, or computer network without authorization or who, having accessed any computer, computer system, computer software, or computer network with authorization, knowingly and intentionally exceeds the limits of such authorization shall be guilty of a Class IV felony if he or she

intentionally:

(1) Deprives another of property or services; or

(2) obtains property or services of another, except that any person who obtains property or services or deprives another of property or services with a value of one thousand dollars or more by such conduct shall be guilty of a Class III felony.

§28-1345. Unlawful acts; harming or disrupting operations; penalties.

Any person who accesses or causes to be accessed any computer, computer system, computer software, or computer network without authorization or who, having accessed any computer, computer system, computer software, or computer network with authorization, knowingly and intentionally exceeds the limits of such authorization shall be guilty of a Class IV felony if he or she intentionally:

(1) Alters, damages, deletes, or destroys any computer, computer system, computer software, computer network, computer program, data, or other property;

(2) disrupts the operation of any computer, computer system, computer software, or computer network; or

(3) distributes a destructive computer program with intent to damage or destroy any computer, computer system, computer network, or computer software, except that any person who causes loss with a value of one thousand dollars or more by such conduct shall be guilty of a Class III felony.

§28-1346. Unlawful acts; obtaining confidential public information; penalties.

Any person who intentionally accesses or causes to be accessed any computer, computer system, computer software, or computer network without authorization, or who, having accessed a computer, computer system, computer software, or computer network with authorization, knowingly and intentionally exceeds the limits of such authorization, and thereby obtains information filed by the public with the state or any political subdivision which is by statute required to be kept confidential shall be guilty of a Class II misdemeanor. For any second or subsequent offense under this section, such person shall be guilty of a Class I misdemeanor.

§28-1347. Unlawful acts; access without authorization; exceeding authorization; penalties.

Any person who intentionally accesses any computer, computer system, computer software, computer network, computer program, or data without authorization and with knowledge that such access was not authorized or who, having accessed any computer, computer system, computer software, computer network, computer program, or data with authorization, knowingly and intentionally exceeds the limits of such authorization shall be guilty of a Class V misdemeanor. For any second or subsequent offense under this section, such person shall be guilty of a Class II misdemeanor.

§28-1348. Act, how construed.

The Computer Crimes Act shall not be construed to preclude the applicability of any other provision of the Nebraska Criminal Code which may apply to any transaction described in the Computer Crimes Act.

NEVADA REVISED STATUTES

TITLE 15. CRIMES AND PUNISHMENTS.
CHAPTER 205. CRIMES AGAINST PROPERTY.
Unlawful Acts Regarding Computers

205.473. Definitions.

As used in NRS 205.473 to 205.491, inclusive, unless the context otherwise requires, the words and terms defined in NRS 205.4732 to 205.476, inclusive, have the meanings ascribed to them in those sections.

205.4732. "Access" defined.

"Access" means to intercept, instruct, communicate with, store data in, retrieve from or otherwise make use of any resources of a computer, network or data.

205.4735. "Computer" defined.

"Computer" means an electronic device which performs logical, arithmetic and memory functions by manipulations of electronic or magnetic impulses and includes all equipment related to the computer in a system or network.

205.474. "Data" defined.

"Data" means a representation in any form of information, knowledge, facts, concepts or instructions which is being prepared or has been formally prepared and is intended to be processed, is being processed or has been processed in a system or network.

205.4745. "Network" defined.

"Network" means a set of related, remotely connected devices and facilities, including more than one system, with the capability to transmit data among them.

205.475. "Program" defined.

"Program" means an ordered set of data representing coded instructions or statements which can be executed by a computer and cause the computer to perform one or more tasks.

NOTES

State owned computer programs not public property. -- Computer programs are intellectual property owned or licensed by the state and are not public records. Although most information stored by computer will, as with other forms of agency records, consist of public records, public inspection of particular information will still be subject to case-by-case analysis. AGO 89-1 (2-6-1989).

Computer programs as property subject to theft. 18 A.L.R.3d 1121.

205.4755. "Property" defined.

"Property" means anything of value and includes a financial instrument, information, electronically produced data, program and any other tangible or intangible item of value.

205.476. "System" defined.

"System" means a set of related equipment, whether or not connected, which is used with or for a computer.

205.4765. Unlawful acts: Generally.

1. Except as otherwise provided in subsection 5, a person who knowingly, willingly and without authorization:

   (a) Modifies;
   (b) Damages;
   (c) Destroys;
   (d) Discloses;
   (e) Uses;
   (f) Transfers;
   (g) Conceals;
   (h) Takes;
   (i) Retains possession of;
   (j) Copies;

(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed; or
(l) Enters,

data, a program or any supporting documents which exist inside or outside a computer, system or network is guilty of a misdemeanor.

2. Except as otherwise provided in subsection 5, a person who knowingly, willingly and without authorization:

(a) Modifies;
(b) Destroys;
(c) Uses;
(d) Takes;
(e) Damages;
(f) Transfers;
(g) Conceals;
(h) Copies;
(i) Retains possession of; or
(j) Obtains or attempts to obtain access to, permits access to or causes to be accessed,

equipment or supplies that are used or intended to be used in a computer, system or network is guilty of a misdemeanor.

3. Except as otherwise provided in subsection 5, a person who knowingly, willingly and without authorization:

(a) Destroys;
(b) Damages;
(c) Takes;
(d) Alters;
(e) Transfers;
(f) Discloses;
(g) Conceals;
(h) Copies;
(i) Uses;
(j) Retains possession of; or
(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed,

a computer, system or network is guilty of a misdemeanor.

4. Except as otherwise provided in subsection 5, a person who knowingly, willingly and without authorization:

(a) Obtains and discloses;
(b) Publishes;
(c) Transfers; or
(d) Uses,

a device used to access a computer, network or data is guilty of a misdemeanor.

5. If the violation of any provision of this section:

(a) Was committed to devise or execute a scheme to defraud or illegally obtain property;
(b) Caused damage in excess of $500; or

(c) Caused an interruption or impairment of a public service, such as a governmental operation, system of public communication or transportation or supply of water, gas or electricity,

the person shall be punished by imprisonment in the state prison for not less than 1 year nor more than 6 years, and may be further punished by a fine of not more than $100,000.

205.477. Unlawful interference with or denial of access or use; unlawful use.

1. Except as otherwise provided in subsection 3, a person who knowingly, willfully and without authorization interferes with, denies or causes the denial of access to or the use of a computer, system or network to a person who has the duty and right to use it is guilty of a misdemeanor.

2. Except as otherwise provided in subsection 3, a person who knowingly, willingly and without authorization uses or causes the use of a computer, system or network to:

(a) Obtain personal information about another person; or

(b) Enter false information about another person to wrongfully damage or enhance that person's credit rating,

is guilty of a misdemeanor.

3. If the violation of subsection 1 or 2 was committed to devise or execute a scheme to defraud or illegally obtain property, the person shall be punished by imprisonment in the state prison for not less than 1 year nor more than 6 years, and may be further punished by a fine of not more than $100,000.

205.480. Transferred.

NOTE

This section is now compiled as NRS 205.920.

205.481. Forgery by creation, alteration or deletion of data.

A person who knowingly, willfully and without authorization creates, alters or deletes any data contained in any computer, system or network which, if done on a written or printed document or instrument, would constitute forgery pursuant to NRS 205.090 or 205.095, is guilty of forgery and shall be punished as provided in NRS 205.090.

205.485. Presumption of authority of employee.

An employee is presumed to have the authority to access and use any computer, network, supporting documents, program or data owned or operated by his employer unless the presumption is overcome by clear and convincing evidence to the contrary.

205.490. Transferred.

NOTE

This section is now compiled as NRS 205.930.

205.491. Enforcement of provisions.

1. If it appears that a person has engaged in or is about to engage in any act or practice which violates any provisions of NRS 205.473 to 205.485, inclusive, the attorney general or the appropriate district attorney may file an action in any court of competent jurisdiction to prevent the occurrence or continuance of that act or practice.

2. An injunction:

   (a) May be issued without proof of actual damage sustained by any person.

   (b) Does not preclude the criminal prosecution and punishment of a violator.

NEW HAMPSHIRE STATUTES ANNOTATED

TITLE LXII. CRIMINAL CODE
CHAPTER 638. FRAUD
COMPUTER CRIME

638:16. Computer Crime; Definitions

For the purpose of this subdivision:

I. "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

II. "Computer" means a programmable, electronic device capable of accepting and processing data.

III. "Computer network" means

(a) a set of related devices connected to a computer by communications facilities, or

(b) a complex of 2 or more computers, including related devices, connected by communications facilities.

IV. "Computer program" means a set of instructions, statements, or related data that, in actual or modified form, is capable of causing a computer or computer system to perform specified functions.

V. "Computer services" includes, but is not limited to, computer access, data processing, and data storage.

VI. "Computer software" means one or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation.

VII. "Computer system" means a computer, its software, related equipment, communications facilities, if any, and includes computer networks.

VIII. "Data" means information of any kind in any form, including computer software.

IX. "Person" means a natural person, corporation, trust, partnership, incorporated or unincorporated association, and any other legal or governmental entity, including any state or municipal entity or public official.

X. "Property" means anything of value, including data.

638:17. Computer Related Offenses

I. A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he knowingly accesses or causes to be accessed any computer system without authorization. It shall be an affirmative defense to a prosecution for unauthorized access to a computer system that:

(a) The person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, had authorized him to access; or

(b) The person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, would have authorized him to access without payment of any consideration; or

(c) The person reasonably could not have known that his access was unauthorized.

II. A person is guilty of the computer crime of theft of computer services when he knowingly accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the purpose of obtaining unauthorized computer services.

III. A person is guilty of the computer crime of interruption of computer services when he, without authorization, knowingly or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.

IV. A person is guilty of the computer crime of misuse of computer system information when:

(a) As a result of his accessing or causing to be accessed a computer system, he knowingly makes or causes to be made an unauthorized display, use, disclosure, or copy, in any form, of data residing in, communicated by, or produced by a computer system; or

(b) He knowingly or recklessly and without authorization:

(1) Alters, deletes, tampers with, damages, destroys, or takes data intended for use by a computer system, whether residing within or external to a computer system;

or

(2) Intercepts or adds to data residing within a computer system; or

(c) He knowingly receives or retains data obtained in violation of subparagraph (a) or nb) of this paragraph; or

(d) He knowingly uses or discloses any data he knows or believes was obtained in violation of subparagraph (a) or nb) of this paragraph.

V. A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, knowingly or recklessly tampers with, takes, transfers, conceals, alters, damages, or destroys any equipment used in a computer system or knowingly or recklessly causes any of the foregoing to occur.

638:18. Computer Crime Penalties

I. Computer crime constitutes a class A felony if the damages to or the value of the property or computer services exceeds $1,000.

II. Computer crime constitutes a class B felony if:

(a) The damage to or the value of the property or computer services exceeds $500; or

(b) The person recklessly engages in conduct which creates a risk of serious physical injury to another person.

III. Computer crime is a misdemeanor if the damage to or the value of the property or computer services, if any, is $500 or less.

IV. If a person has gained money, property, or services or other consideration through the commission of any offense under RSA 638:17, upon conviction thereof, the court, in addition to any sentence of imprisonment or other form of sentence authorized by RSA 651, may, in lieu of imposing a fine, sentence the defendant to pay an amount, fixed by the court, not to exceed double the amount of the defendant's gain from the commission of such offense. In such case, the court shall make a finding as to the amount of the defendant's gain from the offense and, if the record does not contain sufficient evidence to support such finding, the court may conduct a hearing upon the issue. For

the purpose of this section, "gain" means the amount of money or the value of property or computer services or other consideration derived.

V. For the purposes of this section:

(a) The value of property or computer services shall be:

(1) The market value of the property or computer services at the time of the violation; or

(2) If the property or computer services are unrecoverable, damaged, or destroyed as a result of a violation of RSA 638:17 the cost of reproducing or replacing the property or computer services at the time of the violation.

(b) Amounts included in violations of RSA 638:17 committed pursuant to one scheme or course of conduct, whether from the same person or several persons, may be aggregated in determining the grade of the offense.

(c) When the value of the property or computer services or damage thereto cannot be satisfactorily ascertained, the value shall be deemed to be $250.

638:19. Venue

I. In any prosecution for a violation of RSA 638:17 the offense shall be deemed to have been committed in the town in which the act occurred or in which the computer system or part thereof involved in the violation was located.

II. In any prosecution for a violation of RSA 638:17 based upon more than one act in violation thereof, the offense shall be deemed to have been committed in any of the towns in which any of the acts occurred or in which a computer system or part thereof involved in a violation was located.

III. If any act performed in furtherance of the offenses prohibited by RSA 638:17 occurs in this state or if any computer system or part thereof accessed in violation of RSA 638:17 is located in this state, the offense shall be deemed to have occurred in this state.

NEW JERSEY STATUTES ANNOTATED

TITLE 2A. ADMINISTRATION OF CIVIL AND CRIMINAL JUSTICE
SUBTITLE 6. SPECIFIC CIVIL ACTIONS
CHAPTER 38A. COMPUTER SYSTEM

2A:38A-1. Definitions

As used in this act:

a. "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

b. "Computer" means an electronic device or another similar device capable of executing a computer program, including arithmetic, logic, memory or input-output operations, by the manipulation of electronic or magnetic impulses and includes all computer equipment connected to such a device in a computer system or network.

c. "Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

d. "Computer network" means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

e. "Computer program" means a series of instructions or statements executable on a computer, which directs the computer system in a manner to produce a desired result.

f. "Computer software" means a set of computer programs, data, procedures, and associated documentation concerned with the operation of a computer system.

g. "Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

h. "Data" means information, facts, concepts, or instructions prepared for use in a computer, computer system, or computer network.

i. "Data base" means a collection of data.

j. "Financial instrument" includes but is not limited to a check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization

mechanism, marketable security and any computer representation of these items.

k. "Property" includes but is not limited to financial instruments, information, data, and computer software, in either human readable or computer readable form, copies or originals, and any other tangible or intangible item of value.

l. "Services" includes but is not limited to the use of a computer system, computer network, computer programs, data prepared for computer use and data contained within a computer system or computer network.

2A:38A-3. Computer-related offenses; compensatory and punitive damages; costs and expenses

A person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor in the Superior Court and may recover compensatory and punitive damages and the cost of the suit, including a reasonable attorney's fee, costs of investigation and litigation:

a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;

c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;

d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or

e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

NEW JERSEY STATUTES ANNOTATED

TITLE 2C. THE NEW JERSEY CODE OF CRIMINAL JUSTICE
SUBTITLE 2. DEFINITION OF SPECIFIC OFFENSES
PART 2. OFFENSES AGAINST PROPERTY
CHAPTER 20. THEFT AND RELATED OFFENSES
II. COMPUTER-RELATED CRIMES

2C:20-23. Definitions

As used in this act:

a. "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

b. "Computer" means an electronic device or another similar device capable of executing a computer program, including arithmetic, logic, memory or input-output operations, by the manipulation of electronic or magnetic impulses and includes all computer equipment connected to such a device in a computer system or network.

c. "Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

d. "Computer network" means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

e. "Computer program" means a series of instructions or statements executable on a computer, which directs the computer system in a manner to produce a desired result.

f. "Computer software" means a set of computer programs, data, procedures, and associated documentation concerned with the operation of a computer system.

g. "Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

h. "Data" means information, facts, concepts, or instructions prepared for use in a computer, computer system, or computer network.

i. "Data base" means a collection of data.

j. "Financial instrument" includes but is not limited to a check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security and any computer representation of these items.

k. "Services" includes but is not limited to the use of a computer system, computer network, computer programs, data prepared for computer use and data contained within a computer system or computer network.

2C:20-24. Value of property or services

For the purposes of this act, the value of any property or services, including the use of computer time, shall be their fair market value, if it is determined that a willing buyer and willing seller exist. Alternatively, value shall include but not be limited to the cost of generating or obtaining data and storing it within a computer or computer system.

2C:20-25. Computer-related theft

A person is guilty of theft if he purposely or knowingly and without authorization:

a. Alters, damages, takes or destroys any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. Alters, damages, takes or destroys a computer, computer system or computer network;

c. Accesses or attempts to access any computer, computer system or computer network for the purpose of executing a scheme to defraud, or to obtain services, property, or money, from the owner of a computer or any third party; or

d. Alters, tampers with, obtains, intercepts, damages or destroys a financial instrument.

2C:20-26. Property or services of $75,000 or more; degree of crime

a. Theft under section 4 of this act [FN1] constitutes a crime of the second degree if the offense

results in the altering, damaging, destruction or obtaining of property or services with a value of $75,000.00 or more. It shall also be a crime of the second degree if the offense results in a substantial interruption or impairment of public communication, transportation, supply of water, gas or power, or other public service.

b. A person is guilty of a crime of the third degree if he purposely or knowingly accesses and recklessly alters, damages, destroys or obtains any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network with a value of $75,000.00 or more.

2C:20-27. Property or services between $500 and $75,000; degree of crime

a. Theft under section 4 of this act [FN1] constitutes a crime of the third degree if the offense results in the altering, damaging, destruction, or obtaining of property or services with a value of at least $500.00 but less than $75,000.00.

b. A person is guilty of a crime of the fourth degree if he purposely or knowingly accesses and recklessly alters, damages, destroys or obtains any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network with a value of at least $500.00 but less than $75,000.00.

2C:20-28. Property or services between $200 and $500; degree of crime

a. Theft under section 4 of this act [FN1] constitutes a crime of the fourth degree if the offense results in the altering, damaging, destruction or obtaining of property or services with a value of more than $200.00 but less than $500.00.

b. A person is guilty of a disorderly persons offense if he purposely or knowingly accesses and recklessly alters, damages, destroys or obtains any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network with a value of more than $200.00 but less than $500.00.

2C:20-29. Property or services of $200 or less; disorderly persons offense

a. Theft under section 4 of this act [FN1] constitutes a disorderly persons offense when the offense

results in the altering, damaging, destruction or obtaining of property or services with a value of $200.00 or less.

b. A person is guilty of a petty disorderly persons offense if he purposely or knowingly accesses and recklessly alters, damages, destroys or obtains any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network with a value of $200.00 or less.

2C:20-30. Damage or wrongful access to computer system; no assessable damage; degree of crime

A person is guilty of a crime of the third degree if he purposely and without authorization accesses, alters, damages or destroys a computer system or any of its parts, where the accessing and altering cannot be assessed a monetary value or loss.

2C:20-31. Disclosure of data from wrongful access; no assessable damage; degree of crime

A person is guilty of a crime of the third degree if he purposely and without authorization accesses a computer system or any of its parts and directly or indirectly discloses or causes to be disclosed data, data base, computer software or computer programs, where the accessing and disclosing cannot be assessed a monetary value or loss.

2C:20-32. Wrongful access to computer; lack of damage or destruction; disorderly persons offense

A person is guilty of a disorderly persons offense if he purposely and without authorization accesses a computer or any of its parts and this action does not result in the altering, damaging or destruction of any property or services.

2C:20-33. Copy or alteration of program or software with value of $1,000 or less

The copying or altering of a computer program or computer software shall not constitute theft for the purposes of chapters 20 and 21 of Title 2C of the New Jersey Statutes or any offense under this act if the computer program or computer software is of a retail value of $1,000.00 or less and is not copied for

resale.

2C:20-34. Situs of offense

For the purpose of prosecution under this act, the situs of an offense of theft shall be the location of the computer which is accessed, or where the terminal used in the offense is situated, or where the actual damage occurs.

NEW MEXICO STATUTES 1978, ANNOTATED

CHAPTER 30. Criminal Offenses
ARTICLE 45. Computer Crimes

30-45-1 Short title.

This act [30-45-1 to 30-45-7 NMSA 1978] may be cited as the "Computer Crimes Act".

30-45-2 Definitions.

As used in the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978]:

A. "access" means to program, execute programs on, intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any computer resources, including data or programs of a computer, computer system, computer network or database;

B. "computer" includes an electronic, magnetic, optical or other high-speed data processing device or system performing logical, arithmetic or storage functions and includes any property, data storage facility or communications facility directly related to or operating in conjunction with such device or system. The term does not include an automated typewriter or typesetter or a single display machine in and of itself, designed and used solely within itself for word processing, or a portable hand-held calculator, or any other device which might contain components similar to those in computers but in which the components have the sole function of controlling the device for the single purpose for which the device is intended;

C. "computer network" means the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers;

D. "computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from a computer system;

E. "computer property" includes a financial instrument, data, databases, computer software, computer programs, documents associated with computer systems and computer programs, or copies, whether tangible or intangible, and data while in transit;

F. "computer service" includes computer time, the use of the computer system, computer network, computer programs or data prepared for computer use, data contained within a computer network and data processing and other functions performed, in whole or in part, by the use of computers,

computer systems, computer networks or computer software;

G. "computer software" means a set of computer programs, procedures and associated documentation concerned with the operation and function of a computer system;

H. "computer system" means a set of related or interconnected computer equipment, devices and software;

I. "data" means a representation of information, knowledge, facts, concepts or instructions which are prepared and are intended for use in a computer, computer system or computer network;

J. "database" means any data or other information classified, processed, transmitted, received, retrieved, originated, switched, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer system, computer network or computer software; and

K. "financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction, authorization mechanism, marketable security or any other computerized representation thereof.

30-45-3 Computer access with intent to defraud or embezzle.

Any person who knowingly and willfully accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to obtain, by means of embezzlement or false or fraudulent pretenses, representations or promises, money, property or anything of value, where:

A. the money, property or other thing has a value of one hundred dollars ($100) or less is guilty of a petty misdemeanor;

B. the money, property or other thing has a value of more than one hundred dollars ($100) but not more than two hundred fifty dollars ($250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

C. the money, property or other thing has a value of more than two hundred fifty dollars ($250) but not more than two thousand five hundred dollars ($2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

D. the money, property or other thing has a value of more than two thousand five hundred dollars ($2,500) but not more than twenty thousand dollars ($20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

E. the money, property or other thing has a value of more than twenty thousand dollars ($20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-4 Computer abuse.

Any person who knowingly, willfully and without authorization, or having obtained authorization:

A. directly or indirectly alters, changes, damages, disrupts or destroys any computer, computer network, computer property, computer service or computer system where:

(1) the damage to the computer property or computer service has a value of one hundred dollars ($100) or less is guilty of a petty misdemeanor;

(2) the damage to the computer property or computer service has a value of more than one hundred dollars ($100) but not more than two hundred fifty dollars ($250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

(3) the damage to the computer property or computer service has a value of more than two hundred fifty dollars ($250) but not more than two thousand five hundred dollars ($2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

(4) the damage to the computer property or computer service has a value of more than two thousand five hundred dollars ($2,500) but not more than twenty thousand dollars ($20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

(5) the damage to the computer property or computer service has a value of more than twenty thousand dollars ($20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

B. directly or indirectly introduces or causes to be introduced data which the person knows to be false into a computer, computer system, computer network, computer software, computer program, database or any part thereof with the intent of harming the property or financial interests or rights of any person is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-5 Unauthorized computer use.

Any person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity such authorization provides for purposes to which the authorization does not extend, directly or indirectly accesses, uses, takes, transfers, conceals, obtains, copies, or retains possession of any computer, computer network, computer property, computer service, computer system or any part thereof where:

A. the damage to the computer property or computer service has a value of one hundred dollars ($100) or less is guilty of a petty misdemeanor;

B. the damage to the computer property or computer service has a value of more than one hundred dollars ($100) but not more than two hundred fifty dollars ($250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

C. the damage to the computer property or computer service has a value of more than two hundred fifty dollars ($250) but not more than two thousand five hundred dollars ($2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

D. the damage to the computer property or computer service has a value of more than two thousand five hundred dollars ($2,500) but not more than twenty thousand dollars ($20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

E. the damage to the computer property or computer service has a value of more than twenty thousand dollars ($20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-6 Prosecution.

A. Prosecution pursuant to the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978] shall not prevent any prosecutions pursuant to any other provisions of the law where such conduct also constitutes a violation of that other provision.

B. A person found guilty of violating any provision of the Computer Crimes Act shall, in addition to any other punishment, be ordered to make restitution for any financial loss sustained by anyone injured as the direct result of the commission of the crime. Restitution shall be imposed in addition to incarceration, forfeiture or fine, and not in lieu thereof, and may be made a condition of probation. The defendant's present and future ability to make such restitution shall be considered. In an extraordinary case, the court may determine that the interests of those injured and justice would not be served by ordering restitution. In such a case, the court shall make and enter specific written findings on the record substantiating the extraordinary circumstance presented upon which the court determined not to order restitution. In all other cases, the court shall determine the amount and method of restitution.

30-45-7 Forfeiture of property.

A. The following are subject to forfeiture:

(1) all computer property, equipment or products of any kind which have been used, manufactured, acquired or distributed in violation of the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978];

(2) all materials, products and equipment of any kind which are used or intended for use in manufacturing, using, accessing, altering, disrupting, copying, concealing, destroying, transferring, delivering, importing or exporting any computer property or computer service in violation of the Computer Crimes Act;

(3) all books, records and research products and materials involving formulas, microfilm, tapes and data which are used or intended for use in violation of the Computer Crimes Act;

(4) all conveyances, including aircraft, vehicles or vessels, which are used or intended for use to transport or in any manner to facilitate the transportation of property described in Subsection A, B or C of this section for the purpose of violating the Computer Crimes Act;

(5) all property, real, personal or mixed, which has been used or intended for use, maintained or acquired in violation of the Computer Crimes Act; and

(6) all money or proceeds that constitute an instrumentality or derive from a violation of the Computer Crimes Act.

B. Notwithstanding the provisions of Paragraphs (1) through (6) of Subsection A of this section:

(1) no conveyance used by any person as a common carrier in the transaction of business as a common carrier is subject to forfeiture under this section unless it appears that the owner or other person in charge of the conveyance is a consenting party to a violation of the Computer Crimes Act;

(2) no conveyance, computer property, equipment or other material is subject to forfeiture under this section by reason of any act or omission established by the owner to have been committed or omitted without his knowledge or consent;

(3) a conveyance, computer property, equipment or other material is not subject to forfeiture for a violation of law the penalty for which is a misdemeanor or petty misdemeanor; and

(4) a forfeiture of a conveyance, computer property, equipment or material encumbered by a bona fide security interest shall be subject to the interest of a secured party if the secured party neither had knowledge of nor consented to the act or omission.

C. Property subject to forfeiture and disposal under the Computer Crimes Act may be seized by any law enforcement officer upon an order issued by the district court having jurisdiction.

D. Seizure without such an order may be made if:

(1) the seizure is incident to an arrest or search under a search warrant;

(2) the property subject to seizure had been the subject of a prior judgment in favor of the state in an injunction or forfeiture proceeding based upon the Computer Crimes Act; or

(3) the enforcement officer has probable cause to believe that the property, whether real, personal or mixed, was used or intended for use, maintained or acquired in violation of the Computer Crimes Act.

E. In the event of a seizure pursuant to Subsection C or Subsection D of this section, a proceeding under the Computer Crimes Act and the rules of civil procedure for the district courts shall be instituted promptly and not later than thirty days after seizure. The proceeding to forfeit property

under the Computer Crimes Act is against the property and not against the owner or any other person. It is in rem wholly and not in personam. It is a civil case and not a criminal proceeding. The forfeiture proceeding is required, not to complete the forfeiture, but to prove the illegal use for which the forfeiture was suffered.

F. Except as otherwise specifically provided by law, whenever any property is forfeited to the state by reason of the violation of any law, the court by which the offender is convicted shall order the sale or other disposition of the property and the proceeds of any such sale as provided for in this section are subject to the court making due provisions for the rights of innocent persons and the legitimate rights to restitution on behalf of actual victims of the criminal acts.

G. Property taken or detained under this section shall not be subject to replevin but is deemed to be in the custody of the law enforcement agency seizing it subject only to the orders and decrees of the district court. When property is seized under the Computer Crimes Act, the enforcement officer may:

(1) place the property under seal;

(2) remove the property to a place designated by the law enforcement officer or by the district court; or

(3) require the law enforcement agency to take custody of the property and remove it to an appropriate location for disposition in accordance with law.

H. When property is forfeited under the Computer Crimes Act, the law enforcement agency seizing it shall:

(1) deliver custody of the property to the information systems council attached to the general services department. The council, based upon a plan, shall advertise and make available the forfeited property to stated agencies and political subdivisions of the state based upon a demonstrated need and plan of use for that property. The information systems council shall advertise and make the forfeited property available by bid for a minimum of one hundred twenty days and dispose of that property within another sixty days. All proceeds from the sale of forfeited property shall be deposited in the general fund; or

(2) where the court orders the property to be sold, the proceeds of the sale shall be paid into the general fund.

LAWS OF NEW YORK ANNOTATED

CRIMINAL PROCEDURE LAW
CHAPTER 11-A OF THE CONSOLIDATED LAWS
PART TWO--THE PRINCIPAL PROCEEDINGS
TITLE J--PROSECUTION OF INDICTMENTS IN SUPERIOR COURTS
PLEA TO SENTENCE
ARTICLE 250--PRE-TRIAL NOTICES OF DEFENSES

§250.30 Notice of defenses in offenses involving computers

1. In any prosecution in which the defendant seeks to invoke any of the defenses specified in section 156.50 of the penal law, the defendant must within forty-five days after arraignment and not less than twenty days before the commencement of the trial serve upon the people and file with the court a written notice of his intention to present such defense. For good cause shown, the court may extend the period for service of the notice.

2. The notice served must specify the subdivision or subdivisions upon which the defendant relies and must also state the reasonable grounds that led the defendant to believe that he had the authorization required by the statute or the right required by the statute to engage in such conduct.

3. If at the trial the defendant seeks to invoke any of the defenses specified in section 156.50 of the penal law without having served the notice as required, or seeks to invoke a subdivision or a ground not specified in the notice, the court may exclude any testimony or evidence in regard to the defense, or any subdivision or ground, not noticed. The court may in its discretion, for good cause shown, receive such testimony or evidence, but before doing so, it may, upon application of the people, grant an adjournment.

NOTE

Computer Crime is defined as a "serious offense" in General Business Law, Article 7-A- Security Guard Act, §89-f(13).

LAWS OF NEW YORK ANNOTATED

PENAL LAW
CHAPTER 40 OF THE CONSOLIDATED LAWS
PART THREE--SPECIFIC OFFENSES
TITLE J--OFFENSES INVOLVING THEFT
ARTICLE 155--LARCENY

§155.00 Larceny; definitions of terms

The following definitions are applicable to this title:

1. "Property" means any money, personal property, real property, computer data, computer program, thing in action, evidence of debt or contract, or any article, substance or thing of value, including any gas, steam, water or electricity, which is provided for a charge or compensation.

2. "Obtain" includes, but is not limited to, the bringing about of a transfer or purported transfer of property or of a legal interest therein, whether to the obtainer or another.

3. "Deprive." To "deprive" another of property means

   (a) to withhold it or cause it to be withheld from him permanently or for so extended a period or under such circumstances that the major portion of its economic value or benefit is lost to him, or

   (b) to dispose of the property in such manner or under such circumstances as to render it unlikely that an owner will recover such property.

4. "Appropriate." To "appropriate" property of another to oneself or a third person means

   (a) to exercise control over it, or to aid a third person to exercise control over it, permanently or for so extended a period or under such circumstances as to acquire the major portion of its economic value or benefit, or

   (b) to dispose of the property for the benefit of oneself or a third person.

5. "Owner." When property is taken, obtained or withheld by one person from another person, an "owner" thereof means any person who has a right to possession thereof superior to that of the taker, obtainer or withholder. A person who has obtained possession of property by theft or other illegal means shall be deemed to have a right of possession superior to that of a person who takes, obtains or withholds it from him by larcenous means. A joint or common owner of property shall

not be deemed to have a right of possession thereto superior to that of any other joint or common owner thereof. In the absence of a specific agreement to the contrary, a person in lawful possession of property shall be deemed to have a right of possession superior to that of a person having only a security interest therein, even if legal title lies with the holder of the security interest pursuant to a conditional sale contract or other security agreement.

6. "Secret scientific material" means a sample, culture, micro-organism, specimen, record, recording, document, drawing or any other article, material, device or substance which constitutes, represents, evidences, reflects, or records a scientific or technical process, invention or formula or any part or phase thereof, and which is not, and is not intended to be, available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent, and when it accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.

7. "Credit card" means any instrument or article defined as a credit card in section five hundred eleven of the general business law.

7-a. "Debit card" means any instrument or article defined as a debit card in section five hundred eleven of the general business law.

7-b. "Medical assistance card" means an identification card given to an individual for use in securing medical assistance in accordance with title eleven of article five of the social services law.

7-c. "Access device" means any telephone calling card number, credit card number, account number or personal identification number that can be used to obtain telephone service.

8. "Service" includes, but is not limited to, labor, professional service, a computer service, transportation service, the supplying of hotel accommodations, restaurant services, entertainment, the supplying of equipment for use, and the supplying of commodities of a public utility nature such as gas, electricity, steam and water. A ticket or equivalent instrument which evidences a right to receive a service is not in itself service but constitutes property within the meaning of subdivision one.

9. "Cable television service" means any and all services provided by or through the facilities of any cable television system or closed circuit coaxial cable communications system, or any microwave or similar transmission service used in connection with any cable television system or other similar closed circuit coaxial cable communications system.

SELECTED LEGISLATIVE HISTORY

An expired credit card, or any other type of defective credit card, falls within meaning of "credit card" as used in felony statutes relating to larceny and criminal possession of stolen property and, as a matter of reality and practicality, still "may be used" in the same manner as a currently valid one to secure any of the enumerated benefits. People v. Timmons, 1984, 124 Misc.2d 766, 478 N.Y.S.2d 777.

LAWS OF NEW YORK ANNOTATED

PENAL LAW
CHAPTER 40 OF THE CONSOLIDATED LAWS
PART THREE--SPECIFIC OFFENSES
TITLE J--OFFENSES INVOLVING THEFT
ARTICLE 156--OFFENSES INVOLVING COMPUTERS; DEFINITION OF TERMS

§156.00. Offenses involving computers; definition of terms

The following definitions are applicable to this chapter except where different meanings are expressly specified:

1. "Computer" means a device or group of devices which, by manipulation of electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.

2. "Computer program" is property and means an ordered set of data representing coded instructions or statements that, when executed by computer, cause the computer to process data or direct the computer to perform one or more computer operations or both and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

3. "Computer data" is property and means a representation of information, knowledge, facts, concepts or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

4. "Computer service" means any and all services provided by or through the facilities of any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another.

5. "Computer material" is property and means any computer data or computer program which:

   (a) contains records of the medical history or medical treatment of an identified or readily identifiable individual or individuals. This term shall not apply to the gaining access to or duplication solely of the medical history or medical treatment records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(b) contains records maintained by the state or any political subdivision thereof or any governmental instrumentality within the state which contains any information concerning a person, as defined in subdivision seven of section 10.00 of this chapter, which because of name, number, symbol, mark or other identifier, can be used to identify the person and which is otherwise prohibited by law from being disclosed. This term shall not apply to the gaining access to or duplication solely of records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(c) is not and is not intended to be available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent and which accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.

6. "Uses a computer or computer service without authorization" means the use of a computer or computer service without the permission of, or in excess of the permission of, the owner or lessor or someone licensed or privileged by the owner or lessor after notice to that effect to the user of the computer or computer service has been given by:

(a) giving actual notice in writing or orally to the user; or

(b) prominently posting written notice adjacent to the computer being utilized by the user; or

(c) a notice that is displayed on, printed out on or announced by the computer being utilized by the user. Proof that the computer is programmed to automatically display, print or announce such notice or a notice prohibiting copying, reproduction or duplication shall be presumptive evidence that such notice was displayed, printed or announced.

7. "Felony" as used in this article means any felony defined in the laws of this state or any offense defined in the laws of any other jurisdiction for which a sentence to a term of imprisonment in excess of one year is authorized in this state.

REFERENCES

Discovery; upon demand of defendant in cases involving computer offenses, see CPL 240.20.
Geographical jurisdiction of offense of computer trespass, see CPL 20.60.

§156.05. Unauthorized use of a computer

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

Unauthorized use of a computer is a class A misdemeanor.

SELECTIVE LEGISLATIVE HISTORY

Telephone system constituted a "computer" for purposes of statute prohibiting unauthorized use of a computer. People v. Johnson, 1990, 148 Misc.2d 103, 560 N.Y.S.2d 238.

§156.10. Computer trespass

A person is guilty of computer trespass when he knowingly uses or causes to be used a computer or computer service without authorization and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he thereby knowingly gains access to computer material.

Computer trespass is a class E felony.

§156.20. Computer tampering in the second degree

A person is guilty of computer tampering in the second degree when he uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person.

Computer tampering in the second degree is a class A misdemeanor.

SELECTIVE LEGISLATIVE HISTORY

Issuance of commands to computer software which changed instructions to computer hardware, thereby taking it off its normal course of action in shutting down phone lines run by computer, constituted "alteration" of computer program for purposes of computer tampering statute. People v. Versaggi, 1987, 136 Misc.2d 361, 518 N.Y.S.2d 553.

§156.25. Computer tampering in the first degree

A person is guilty of computer tampering in the first degree when he commits the crime of computer tampering in the second degree and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he has been previously convicted of any crime under this article or subdivision ten of section 165.15 of this chapter; or

3. he intentionally alters in any manner or destroys computer material; or

4. he intentionally alters in any manner or destroys computer data or a computer program in an amount exceeding one thousand dollars.

Computer tampering in the first degree is a class E felony.

§156.30. Unlawful duplication of computer related material

A person is guilty of unlawful duplication of computer related material when having no right to do so, he copies, reproduces or duplicates in any manner:

1. any computer data or computer program and thereby intentionally and wrongfully deprives or appropriates from an owner thereof an economic value or benefit in excess of two thousand five hundred dollars; or

2. any computer data or computer program with an intent to commit or attempt to commit or further the commission of any felony.

Unlawful duplication of computer related material is a class E felony.

§156.35. Criminal possession of computer related material

A person is guilty of criminal possession of computer related material when having no right to do so, he knowingly possesses, in any form, any copy, reproduction or duplicate of any computer data or computer program which was copied, reproduced or duplicated in violation of section 156.30 of this article, with intent to benefit himself or a person other than an owner thereof.

Criminal possession of computer related material is a class E felony.

§156.50. Offenses involving computers; defenses

In any prosecution:

1. under section 156.05 or 156.10 of this article, it shall be a defense that the defendant had reasonable grounds to believe that he had authorization to use the computer;

2. under section 156.20 or 156.25 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to alter in any manner or destroy the computer data or the computer program;

3. under section 156.30 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to copy, reproduce or duplicate in any manner the computer data or the computer program.

GENERAL STATUTES OF NORTH CAROLINA

CHAPTER 14. CRIMINAL LAW.
SUBCHAPTER XI. GENERAL POLICE REGULATIONS.
ARTICLE 60. COMPUTER-RELATED CRIME.

§14-453 Definitions.

As used in this section, unless the context clearly requires otherwise, the following terms have the meanings specified:

(1) "Access" means to approach, instruct, communicate with, cause input, cause output, or otherwise make use of any resources of a computer, computer system or computer network.

(2) "Computer" means an internally programmed, automatic device that performs data processing.

(3) "Computer network" means the interconnection of communication systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data.

(5) "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected computer equipment and devices.

(7) "Financial statement" includes but is not limited to any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card of [or] marketable security, or any electronic data processing representation thereof.

(8) "Property" includes but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing and storage functions.

§14-454 Accessing computers.

(a) A person is guilty of a Class H felony if he willfully, directly or indirectly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof, for the purpose of:

(1) Devising or executing any scheme or artifice to defraud, unless the object of the scheme or artifice is to obtain educational testing material, a false educational testing score, or a false academic or vocational grade, or

(2) Obtaining property or services other than educational testing material, a false educational testing score, or a false academic or vocational grade for himself or another, by means of false or fraudulent pretenses, representations or promises.

(b) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof, for any purpose other than those set forth in subsection (a) above, is guilty of a misdemenor.

§14-455 Damaging computers and related materials.

(a) A person is guilty of a Class H felony if he willfully and without authorization alters, damages or destroys a computer, computer system, computer network, or any part thereof.

(b) A person is guilty of a misdemeanor if he willfully and without authorization alters, damages, or destroys any computer software, program or data residing or existing internal or external to a computer, computer system or computer network.

§14-456 Denial of computer services to an authorized user.

Any person who willfully and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, is guilty of a misdemeanor.

§14-457 Extortion.

Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14-455 with the intent to extort money or any pecuniary advantage, or with the intent

to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony.

NORTH DAKOTA CENTURY CODE

TITLE 12.1. CRIMINAL CODE
CHAPTER 12.1-06.1.
RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS

12.1-06.1-08. Computer fraud -- Computer crime -- Classification -- Penalty.

1. A person commits computer fraud by gaining or attempting to gain access to, altering, damaging, modifying, copying, disclosing, taking possession of, or destroying any computer, computer system, computer network, or any part of such computer, system, or network, without authorization, and with the intent to devise or execute any scheme or artifice to defraud, deceive, prevent the authorized use of, or control property or services by means of false or fraudulent pretenses, representations, or promises. A person who commits computer fraud is guilty of a class C felony.

2. A person commits computer crime by intentionally and either in excess of authorization given or without authorization gaining or attempting to gain access to, altering, damaging, modifying, copying, disclosing, taking possession of, destroying, or preventing the authorized use of any computer, computer system, or computer network, or any computer software, program, or data contained in such computer, computer system, or computer network. A person who commits computer crime is guilty of a class A misdemeanor.

REFERENCES

Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 ALR 4th 971.

What is computer "trade secret" under state law, 53 ALR 4th 1046.

OHIO REVISED CODE ANNOTATED

TITLE 29: CRIMES--PROCEDURE
CHAPTER 2901: GENERAL PROVISIONS
IN GENERAL

§2901.01 Definitions.

As used in the Revised Code:

. . .

(J)

(1) "Property" means any property, real or personal, tangible or intangible, and any interest or license in such property. "Property" includes, but is not limited to, cable television service, computer data, computer software, financial instruments associated with computers, and other documents associated with computers, or copies of the documents, whether in machine or human readable form. "Financial instruments associated with computers" include, but are not limited to, checks, drafts, warrants, money orders, notes of indebtedness, certificates of deposit, letters of credit, bills of credit or debit cards, financial transaction authorization mechanisms, marketable securities, or any computer system representations of any of them.

(2) As used in this division and division (M) of this section, "cable television service," "computer," "computer software," "computer system," " computer network," and "data" have the same meaning as in section 2913.01 of the Revised Code.

. . .

(M) "Contraband" means any property described in the following categories:

. . .

(10) Any computer, computer system, computer network, or computer software that is used in a conspiracy to commit, an attempt to commit, or in the commission of any offense, if the owner of the computer, computer system, computer network, or computer software is convicted of or pleads guilty to the offense in which it is used.

. . .

§2901.12 Venue.

. . .

(I) (1) When the offense involves a computer, computer system, or computer network, the offender may be tried in any jurisdiction containing any location of the computer, computer system, or computer network of the victim of the offense or any jurisdiction in which the alleged offender commits any activity that is an essential part of the offense.

(2) As used in this section, "computer,""computer system," and "computer network"have the same meaning as in section 2913.01 of the Revised Code.

OHIO REVISED CODE ANNOTATED

TITLE 29: CRIMES--PROCEDURE
CHAPTER 2913: THEFT AND FRAUD
IN GENERAL

§2913.01 Definitions.

As used in this chapter:

. . .

(L) "Computer services" includes, but is not limited to, the use of a computer system, computer network, computer program, data that is prepared for computer use, or data that is contained within a computer system or computer network.

(M) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses. " Computer" includes, but is not limited to, all input, output, processing, storage, computer program, or communication facilities that are connected, or related, in a computer system or network to such an electronic device.

(N) "Computer system" means a computer and related devices, whether connected or unconnected, including, but not limited to, data input, output, and storage devices, data communications links, and computer programs and data that make the system capable of performing specified special purpose data processing tasks.

(O) "Computer network"means a set of related and remotely connected computers and communication facilities that includes more than one computer system that has the capability to transmit among the connected computers and communication facilities through the use of computer facilities.

(P) "Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, cause the computer to process data.

(Q) "Computer software" means computer programs, procedures, and other documentation associated with the operation of a computer system.

(R) "Data" means a representation of information, knowledge, facts, concepts, or instructions that are being or have been prepared in a formalized manner and that are intended for use in a computer system or computer network. For purposes of section 2913.47 of the Revised Code, "data" has the additional meaning set forth in division (A) of that section.

(S) "Cable television service" means any services provided by or through the facilities of any cable

television system or other similar closed circuit coaxial cable communications system, or any microwave or similar transmission service used in connection with any cable television system or other similar closed circuit coaxial cable communications system.

(T) "Gain access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(U) "Credit card" includes, but is not limited to, a card, code, device, or other means of access to a customer's account for the purpose of obtaining money, property, labor, or services on credit, or for initiating an electronic fund transfer at a point-of-sale terminal, an automated teller machine, or a cash dispensing machine.

(V) "Electronic fund transfer" has the same meaning as in 92 Stat. 3728, 15 U.S.C.A. 1693a, as amended.

§2913.04 Unauthorized use of property.

(A) No person shall knowingly use or operate the property of another without the consent of the owner or person authorized to give consent.

(B) No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, or computer network without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, or computer network or other person authorized to give consent by the owner.

(C) The affirmative defenses contained in division (C) of section 2913.03 of the Revised Code are affirmative defenses to a charge under this section.

(D) Whoever violates this section is guilty of unauthorized use of property. If the offense involves a violation of division (A) of this section and does not involve any computer, computer system, computer network, computer software, or data, unauthorized use of property is a misdemeanor of the fourth degree. If the offense involves a violation of division (A) of this section and involves any computer, computer system, computer network, computer software, or data or if the offense involves a violation of division (B) of this section, unauthorized use of property is whichever of the following is applicable:

(1) If division (D)(2) or (3) of this section does not apply, a felony of the fourth degree;

(2) If division (D)(3) of this section does not apply and the offender previously has been convicted of a theft offense, a felony of the third degree; (3) If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, a felony of the second degree.

SELECTED LEGISLATIVE HISTORY

In a prosecution for gaining unauthorized access to the computer networks of business, testimony by police computer experts as to the results they obtained in running the confiscated programs and equipment is admissible: State v. Bernatowicz, 62 OApp3d 132, 574 NE2d 1132.

§2913.42 Tampering with records.

(A) No person, knowing he has no privilege to do so, and with purpose to defraud or knowing that he is facilitating a fraud, shall do any of the following:

(1) Falsify, destroy, remove, conceal, alter, deface, or mutilate any writing, data, or record;

(2) Utter any writing or record, knowing it to have been tampered with as provided in division (A)(1) of this section.

(B) No person, knowing he has no privilege to do so, shall falsify, destroy, remove, conceal, alter, deface, or mutilate any computer software or data.

(C) (1) Whoever violates this section is guilty of tampering with records.

(2) If the offense involves a violation of division (A) of this section and does not involve data, tampering with records is whichever of the following is applicable:

(a) If division (C)(2)(b) of this section does not apply, a misdemeanor of the first degree;

(b) If the writing or record is a will unrevoked at the time of the offense or a record kept by or belonging to a governmental agency, a felony of the fourth degree.

(3) If the offense involves a violation of division (A) of this section involving data, tampering with records is whichever of the following is applicable:

(a) If division (C)(3)(b) or (c) of this section does not apply, a felony of the fourth degree;

(b) If division (C)(3)(c) of this section does not apply and the writing or record is a record kept by or belonging to a governmental agency or the offender previously has been convicted of a theft offense, a felony of the third degree;

(c) If the value of the data involved in the offense or the loss to the victim is one hundred dollars or more, a felony of the second degree.

(4) If the offense involves a violation of division (B) of this section, tampering with records is whichever of the following is applicable:

(a) If division (C)(4)(b) or (c) of this section does not apply, a felony of the fourth degree;

(b) If division (C)(4)(c) of this section does not apply and the offender previously has been convicted of a theft offense, a felony of the third degree;

(c) If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, a felony of the second degree.

NOTES

This section prohibits tampering with all private as well as public records, for fraudulent purposes, and thus expands upon former law which prohibited such conduct only with respect to public documents, wills, animal pedigrees, herd registers, and dairy cattle milk production. In general, the rationale for the section is that substantial harm can, in a given case, result from tampering with a personal letter file, bank statement, or other private document, as well as from tampering with the correspondence files or records in a public office. The section recognizes, however, that substantial harm is more likely to result from tampering with wills or public records, and such conduct thus carries a more severe penalty. Any writing or record kept by or belonging to a governmental agency can be the subject of an offense under this section, and the document involved need not

necessarily be a "public record" as defined in section 149.43 of the Revised Code. Tampering with records is a misdemeanor of the first degree. If the writing or record involved in the offense is an unrevoked will or a record kept by or belonging to a governmental agency, tampering with records is a felony of the fourth degree.

§2913.47 Insurance fraud.

(A) As used in this section:

(1) "Data" has the same meaning as in section 2913.01 of the Revised Code and additionally includes any other representation of information, knowledge, facts, concepts, or instructions that are being or have been prepared in a formalized manner.

(2) "Deceptive" means that a statement, in whole or in part, would cause another to be deceived because it contains a misleading representation, withholds information, prevents the acquisition of information, or by any other conduct, act, or omission creates, confirms, or perpetuates a false impression, including, but not limited to, a false impression as to law, value, state of mind, or other objective or subjective fact.

(3) "Insurer" means any person that is authorized to engage in the business of insurance in this state under Title XXXIX [39] of the Revised Code; any prepaid dental plan, medical care corporation, health care corporation, dental care corporation, or health maintenance organization; and any legal entity that is self-insured and provides benefits to its employees or members.

(4) "Policy" means a policy, certificate, contract, or plan that is issued by an insurer.

(5) "Statement" includes, but is not limited to, any notice, letter, or memorandum; proof of loss; bill of lading; receipt for payment; invoice, account, or other financial statement; estimate of property damage; bill for services; diagnosis or prognosis; prescription; hospital, medical, or dental chart or other record; x-ray, photograph, videotape, or movie film; test result; other evidence of loss, injury, or expense; computer-generated document; and data in any form.

(B) No person, with purpose to defraud or knowing that he is facilitating a fraud, shall do either of the following:

(1) Present to, or cause to be presented to, an insurer any written or oral statement that is part of, or in support of, an application for insurance, a claim for payment pursuant to a policy, or a claim for any other benefit pursuant to a policy, knowing that the statement, or any part of the statement, is false or deceptive;

(2) Assist, aid, abet, solicit, procure, or conspire with another to prepare or make any written or oral statement that is intended to be presented to an insurer as part of, or in support of, an application for insurance, a claim for payment pursuant to a policy, or a claim for any other benefit pursuant to a policy, knowing that the statement, or any part of the statement, is false or deceptive.

(C) Whoever violates this section is guilty of insurance fraud. If the false or deceptive statement is presented or intended to be presented as part of, or in support of, an application for insurance or if the amount of the claim that is false or deceptive is less than three hundred dollars, insurance fraud is a misdemeanor of the first degree. If the amount of the claim that is false or deceptive is three hundred dollars or more and is less than five thousand dollars, or if the offender previously has been convicted of a theft offense, insurance fraud is a felony of the fourth degree. If the amount of the claim that is false or deceptive is five thousand dollars or more and is less than one hundred thousand dollars, or if the offender previously has been convicted of two or more theft offenses, insurance fraud is a felony of the third degree. If the amount of the claim that is false or deceptive is one hundred thousand dollars or more, insurance fraud is a felony of the second degree.

(D) This section shall not be construed to abrogate, waive, or modify division (A) of section 2317.02 of the Revised Code.

§2913.81 Denying access to a computer.

(A) No person, without privilege to do so, shall knowingly deny or cause the denial of a computer system or computer services to an authorized user of a computer system or computer services that, in whole or in part, are owned by, under contract to, operated for, or operated in conjunction with another person.

(B) Whoever violates this section is guilty of denying access to a computer, a felony of the fourth degree. If the offender previously has been convicted of a theft offense, denying access to a computer is a felony of the third degree. If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, denying access to a

computer is a felony of the second degree.

§2917.21 Telephone harassment.

(A) No person shall knowingly make or cause to be made a telephone call, or knowingly permit a telephone call to be made from a telephone under his control, to another, if the caller does any of the following:

(1) Fails to identify himself to the recipient of the telephone call and makes the telephone call with purpose to harass, abuse, or annoy any person at the premises to which the telephone call is made, whether or not conversation takes place during the telephone call;

(2) Describes, suggests, requests, or proposes that the caller, recipient of the telephone call, or any other person engage in, any sexual activity as defined in division (C) of section 2907.01 of the Revised Code, and the recipient of the telephone call, or another person at the premises to which the telephone call is made, has requested, in a previous telephone call or in the immediate telephone call, the caller not to make a telephone call to the recipient of the telephone call or to the premises to which the telephone call is made;

(3) During the telephone call, violates section 2903.21 of the Revised Code;

(4) Knowingly states to the recipient of the telephone call that he intends to cause damage to or destroy public or private property, and the recipient of the telephone call, any member of the family of the recipient of the telephone call, or any other person who resides at the premises to which the telephone call is made owns, leases, resides, or works in, will at the time of the destruction or damaging be near or in, has the responsibility of protecting, or insures the property that will be destroyed or damaged;

(5) Knowingly makes the telephone call to the recipient of the telephone call, to another person at the premises to which the telephone call is made, or to the premises to which the telephone call is made, and the recipient of the telephone call, or another person at the premises to which the telephone call is made, has previously told the caller not to call the premises to which the telephone call is made or not to call any persons at the premises to which the telephone call is made.

(B) No person shall make or cause to be made a telephone call, or permit a telephone call to be made from a telephone under his control, with purpose to abuse, threaten, annoy, or harass another

person.

(C) Whoever violates this section is guilty of telephone harassment, a misdemeanor of the first degree. If the offender has previously been convicted of a violation of this section, then telephone harassment is a felony of the fourth degree.

NOTES

This section broadens the prohibition contained in section 4931.31 of the Revised Code, so as to include all seriously vexatious phone calls. The kind of offense defined in the section is extremely annoying or distressing to victims, and offenders are difficult to track down. Police and telephone company personnel regularly spend hundreds of man-hours attempting to apprehend a single offender in cases of this sort. Accordingly, the offense is graded as a serious misdemeanor.

Telephone harassment is a misdemeanor of the first degree.

SELECTED LEGISLATIVE HISTORY

Evidence of ill will between the complainant and the defendant, plus evidence from a computerized "trap" that anonymous, silent harassing calls were made from a single telephone line listed in the names of the defendant and her husband as subscribers, is insufficient to convict the defendant of telephone harassment beyond a reasonable doubt: Dayton v. Glisson, 36 OApp3d 159, 521 NE2d 853.

§ 2917.21(A)(5), which makes it a crime for a person to call a premises, having been previously told by anyone at that premises not to call, is not vague and is, therefore, constitutional: State v. Mollenkopf, 8 OApp3d 210, 8 OBR 281, 456 NE2d 1269.

Computer printouts from the telephone company are admissible under the business records exception of EvR 803(6) in a prosecution under RC s 2917.21, since installing computerized "traps" is a regular business activity of the telephone company's security department and the security department's manager lays a foundation by testifying as to department policies and procedures regarding telephone harassment complaints: State v. Knox, 18 OApp3d 36, 18 OBR 61, 480 NE2d 120.

§2923.24 Possessing criminal tools.

(A) No person shall possess or have under his control any substance, device, instrument, or article, with purpose to use it criminally.

(B) Each of the following constitutes prima-facie evidence of criminal purpose:

(1) Possession or control of any dangerous ordnance, or the materials or parts for making dangerous ordnance, in the absence of circumstances indicating such dangerous ordnance, materials, or parts are intended for legitimate use;

(2) Possession or control of any substance, device, instrument, or article designed or specially adapted for criminal use;

(3) Possession or control of any substance, device, instrument, or article commonly used for criminal purposes, under circumstances indicating such item is intended for criminal use.

(C) Whoever violates this section is guilty of possessing criminal tools, a felony of the fourth degree.

SELECTED LEGISLATIVE HISTORY

The theft in office statute, RC §2921.41, is violated when a defendant aids and abets a public official (a deputy clerk of court) in obtaining confidential information from a Law Enforcement Automated Data System ("LEADS") computer terminal for an unauthorized purpose (checking traffic records of defendant's private insurance clients). Where defendant engages in a common design or purpose to commit a theft offense (obtaining confidential LEADS information for an unauthorized purpose) and the use of a LEADS computer terminal is the sole means by which this information is obtained, he may be convicted of possession of a criminal tool (the computer terminal) as prohibited in RC §2923.24: State v. Haberek, 47 OApp3d 35, 546 NE2d 1361.

§2925.44 Rights of law enforcement agency seizing property; disposition of forfeited property.

(A) If property is seized pursuant to section 2925.42 or 2925.43 of the Revised Code, it is deemed to be in the custody of the head of the law enforcement agency that seized it, and he may do any of the following with respect to that property prior to its disposition in accordance with division (A)(4) or (B) of this section:

(1) Place the property under seal;

(2) Remove the property to a place that he designates;

(3) Request the issuance of a court order that requires any other appropriate municipal corporation, county, township, or state law enforcement officer or other officer to take custody of the property and, if practicable, remove it to an appropriate location for eventual disposition in accordance with division (B) of this section;

(4) Seek forfeiture of the property pursuant to federal law. If the head of the law enforcement agency that seized the property seeks its forfeiture pursuant to federal law, the law enforcement agency shall deposit, use, and account for any proceeds from a sale of the property upon its forfeiture, any proceeds from another disposition of the property upon its forfeiture, or any forfeited moneys it receives, in accordance with the applicable federal law and otherwise shall comply with that law. Division (B) of this section and divisions (D)(1) to (3) of section 2933.43 of the Revised Code do not apply to, and shall not be construed as applying to, any proceeds or forfeited moneys received pursuant to federal law.

(B) In addition to complying with any requirements imposed by a court pursuant to section 2925.42 or 2925.43 of the Revised Code, and the requirements imposed by those sections, in relation to the disposition of property forfeited to the state under either of those sections, the prosecuting attorney who is responsible for its disposition shall dispose of the property as follows:

. . .

(5) Computers, computer networks, computer systems, and computer software suitable for police work may be given to a law enforcement agency for that purpose. Other computers, computer networks, computer systems, and computer software shall be disposed of by sale pursuant to division (B)(8) of this section or disposed of in another manner that the court that issued the order of forfeiture considers proper under the circumstances. As used in this division, "computers," "computer networks," "computer systems," and "computer software" have the same meanings as in section 2913.01 of the Revised Code.

. . .

§2933.52 Interception of wire or oral communications.

(A) No person purposely shall do any of the following:

(1) Intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any wire or oral communication;

(2) Use, attempt to use, or procure any other person to use or attempt to use any interception device to intercept any wire or oral communication, if either of the following apply:

(a) The interception device is affixed to, or otherwise transmits a signal through, a wire, cable, satellite, microwave, or other similar method of connection used in wire communications;

(b) The interception device transmits communications by radio, or interferes with the transmission of communications by radio.

(3) Disclose, or attempt to disclose, to any other person the contents, or any evidence derived from the contents, of any wire or oral communication, knowing or having reason to know that the contents, or evidence derived from the contents, was obtained through the interception of the wire or oral communication in violation of sections 2933.51 to 2933.66 of the Revised Code.

(B) This section does not apply to any of the following:

(1) The interception, disclosure, or use of the contents, or any evidence derived from the contents, of any oral or wire communication that is obtained through the use of an interception warrant issued pursuant to sections 2933.53 to 2933.56 of the Revised Code, that is obtained pursuant to an oral approval for an interception granted pursuant to section 2933.57 of the Revised Code, or that is obtained pursuant to any order or interception that is issued or made in accordance with section 802 of the "Omnibus Crime Control and Safe Streets Act of 1968," 82 Stat. 237, 254, 18 U.S.C. 2510 to 2520 (1968), as amended, or the "Foreign Intelligence Surveillance Act,"92 Stat. 1783, 50 U.S.C. 1801.11 (1978), as amended;

(2) An operator of a switchboard, or an officer or agent of a communications common carrier, whose facilities are used in the transmission of a wire communication to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity that is necessary to the rendition of service or the protection of the rights or property of the communications common carrier, provided that the communications common carrier shall not utilize service observing or random monitoring except for

mechanical or service quality control checks;

(3) A law enforcement officer who intercepts a wire or oral communication, if the officer is a party to the communication or if one of the parties to the communication has given prior consent to the interception by the officer;

(4) A person who is not a law enforcement officer and who intercepts a wire or oral communication, if the person is a party to the communication or if one of the parties to the communication has given the person prior consent to the interception, and if the communication is not intercepted for the purpose of committing any criminal offense or tortious act in violation of the laws or Constitution of the United States or this state or for the purpose of committing any other injurious act;

(5) An officer, employee, or agent of any communications common carrier providing information, facilities, or technical assistance to an investigative officer who is authorized to intercept a wire or oral communication pursuant to sections 2933.51 to 2933.66 of the Revised Code;

(6) A pen register, which, as used in this section, means a device that records or decodes electronic impulses that identify the numbers dialed, pulsed, or otherwise transmitted on telephone lines to which the device is attached;

(7) A trap, which, as used in this section, means any device or apparatus that connects to any telephone or telegraph instrument, equipment, or facility and determines the origin of a wire communication to a telephone or telegraph instrument, equipment or facility, but does not intercept the contents of any wire communication;

(8) Any police, fire, or emergency communications system to intercept wire communications coming into and going out of the communications system of a police department, fire department, or emergency center, if both of the following apply:

(a) The telephone, instrument, equipment, or facility is limited to the exclusive use of the communication system for administrative purposes;
(b) At least one telephone, instrument, equipment, or facility that is not subject to interception is made available for public use at each police department, fire department, or emergency center.

(C) Whoever violates this section is guilty of interception of wire or oral communications, a felony of

the third degree.

OKLAHOMA STATUTES ANNOTATED

TITLE 21. CRIMES AND PUNISHMENTS
PART VII. CRIMES AGAINST PROPERTY
CHAPTER 61. FALSE PRETENSES, FALSE PERSONATIONS, CHEATS AND FRAUDS
CREDIT CARDS

§1550.1. Definitions

1. The term "credit card" means an identification card or device issued to a person, firm or corporation by a business organization which permits such person, firm or corporation to purchase or obtain goods, property or services on the credit of such organization.

2. "Debit card" means an identification card or device issued to a person, firm or corporation by a business organization which permits such person, firm or corporation to obtain access to or activate a consumer banking electronic facility.

Title of Act:

An Act to prohibit obtaining credit by use of a credit card issued to another without consent of the person to whom issued or which has been expired or been cancelled and prescribing penalties therefor; and declaring an emergency. Laws 1961, p. 233.

§1550.2. Prohibitions on use of credit and debit cards--Penalties

Any person who knowingly uses or attempts to use in person or by telephone, for the purpose of obtaining credit, or for the purchase of goods, property or services, or for the purpose of obtaining cash advances in lieu of these items, or to deposit, obtain or transfer funds, either a credit card or a debit card which has not been issued to such person or which is not used with the consent of the person to whom issued or a credit card or a debit card which has been revoked or canceled by the issuer of such card and actual notice thereof has been given to such person, or a credit card or a debit card which is false, counterfeit or nonexistent is guilty of a misdemeanor and punishable by a fine of not more than One Hundred Dollars ($100.00) or imprisonment for not more than thirty (30) days or both such fine and imprisonment if the amount of the credit or purchase or funds deposited, obtained or transferred by such use does not exceed Fifty Dollars ($50.00); or by a fine of not less than One Hundred Dollars ($100.00) nor more than Five Hundred Dollars ($500.00) or imprisonment for not more than one (1) year or both such fine and imprisonment if the amount of the credit or purchase or funds deposited, obtained or transferred by such use exceeds Fifty Dollars ($50.00).

NOTES

Obtaining less than $50 worth of property by use of a stolen credit card was not an act punishable only as a misdemeanor under this section proscribing use of credit cards without consent of owner, but such act was also punishable under § 1577 of this title pertaining to use of forged instrument. Shriver v. Graham, Okl.Cr., 366 P.2d 774 (1962).

OKLAHOMA STATUTES ANNOTATED

TITLE 21. CRIMES AND PUNISHMENTS
PART VII. CRIMES AGAINST PROPERTY
CHAPTER 70. OTHER OFFENSES AGAINST PROPERTY RIGHTS
COMPUTER CRIMES ACT

§1951. Short title

This act shall be known and may be cited as the "Oklahoma Computer Crimes Act".

Title of Act:

An Act relating to crimes and punishments; providing short title; defining terms; prohibiting access to computer, computer system or computer network under certain circumstances; forbidding alteration, damage, destruction or disclosure of certain software or data; providing that proof of certain acts is prima facie evidence; providing penalties; providing for codification; providing severability; and declaring an emergency. Laws 1984, c. 70.

§1952. Definitions

As used in the Oklahoma Computer Crimes Act: [FN1]

1. "Access" means to approach, gain entry to, instruct, communicate with, store data in, retrieve data from or otherwise use the logical, arithmetical, memory or other resources of a computer, computer system or computer network;

2. "Computer" means an electronic device which performs work using programmed instruction having one or more of the capabilities of storage, logic, arithmetic or communication. The term includes input, output, processing, storage, software and communication facilities which are connected or related to a device in a system or network;

3. "Computer network" means the interconnection of terminals by communication modes with a computer, or a complex consisting of two or more interconnected computers;

4. "Computer program" means a set or series of instructions or statements and related data which when executed in actual or modified form directs or is intended to direct the functioning of a computer system in a manner designed to perform certain operations;

5. "Computer software" means one or more computer programs, procedures and associated documentation used in the operation of a computer system;

6. "Computer system" means a set of related, connected or unconnected, computer equipment, devices including support devices, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control and software. "Computer system" does not include calculators which are not programmable and are not capable of being connected to or used to access other computers, computer networks, computer systems or support devices;

7. "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device;

8. "Property" means any tangible or intangible item of value and includes, but is not limited to, financial instruments, geophysical data or the interpretation of that data, information, computer software, computer programs, electronically-produced data and computer-produced or stored data, supporting documentation, computer software in either machine or human readable form, electronic impulses, confidential, copyrighted or proprietary information, private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transactions and telecommunications services or permit electronic fund transfers and any other tangible or intangible item of value;

9. "Services" includes, but is not limited to, computer time, data processing and storage functions and other uses of a computer, computer system or computer network to perform useful work;

10. "Supporting documentation" includes, but is not limited to, all documentation in any form used in the construction, design, classification, implementation, use or modification of computer software, computer programs or data; and

11. "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program or data was or was not altered, deleted, disrupted, damaged or destroyed by the access.

§1953. Prohibited acts

A. It shall be unlawful to:

1. Willfully, and without authorization, gain or attempt to gain access to and damage, modify, alter, delete, destroy, copy, make use of, disclose or take possession of a computer, computer system, computer network or any other property.

2. Use a computer, computer system, computer network or any other property as hereinbefore defined for the purpose of devising or executing a scheme or artifice with the intent to defraud, deceive, extort or for the purpose of controlling or obtaining money, property, services or other thing of value by means of a false or fraudulent pretense or representation.

3. Willfully exceed the limits of authorization and damage, modify, alter, destroy, copy, delete, disclose or take possession of a computer, computer system, computer network or any other property.

4. Willfully and without authorization, gain or attempt to gain access to a computer, computer system, computer network or any other property.

5. Willfully and without authorization use or cause to be used computer services.

6. Willfully and without authorization disrupt or cause the disruption of computer services or deny or cause the denial of access or other computer services to an authorized user of a computer, computer system or computer network.

7. Willfully and without authorization provide or assist in providing a means of accessing a computer, computer system or computer network in violation of this section.

B. Any person convicted of violating paragraphs 1, 2, 3, 6 or 7 of subsection A of this section shall be guilty of a felony.

C. Any person convicted of violating paragraphs 4 or 5 of subsection A of this section shall be guilty of a misdemeanor.

§1954. Certain acts as prima facie evidence of violation of act

Proof that any person has accessed, damaged, disrupted, deleted, modified, altered, destroyed, caused to be accessed, copied, disclosed or taken possession of a computer, computer system, computer network

or any other property, or has attempted to perform any of these enumerated acts without authorization or exceeding the limits of authorization, shall be prima facie evidence of the willful violation of the Oklahoma Computer Crimes Act. [FN1]

§1955. Penalties--Civil actions

A. Upon conviction of a felony under the provisions of the Oklahoma Computer Crimes Act, [FN1] punishment shall be by a fine of not less than Five Thousand Dollars ($5,000.00) and not more than One Hundred Thousand Dollars ($100,000.00), or by confinement in the State Penitentiary for a term of not more than ten (10) years, or by both such fine and imprisonment.

B. Upon conviction of a misdemeanor under the provisions of the Oklahoma Computer Crimes Act, punishment shall be by a fine of not more than Five Thousand Dollars ($5,000.00), or by imprisonment in the county jail not to exceed thirty (30) days, or by both such fine and imprisonment.

C. In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program or data may bring a civil action against any person convicted of a violation of the Oklahoma Computer Crimes Act for compensatory damages, including any victim expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program or data was or was not altered, damaged, deleted, disrupted or destroyed by the access. In any action brought pursuant to this subsection the court may award reasonable attorneys fees to the prevailing party.

§1957. Access of computer, computer system or computer network in one jurisdiction from another jurisdiction--Bringing of action

For purposes of bringing a civil or a criminal action under the Oklahoma Computer Crimes Act, [FN1] a person who causes, by any means, the access of a computer, computer system or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system or computer network in each jurisdiction.

§1958. Access to computers, computer systems and computer networks prohibited for certain purposes--Penalty

No person shall communicate with, store data in, or retrieve data from a computer system or computer network for the purpose of using such access to violate any of the provisions of the Oklahoma Statutes.

Any person convicted of violating the provisions of this section shall be guilty of a felony punishable by imprisonment in the State Penitentiary for a term of not more than five (5) years, or by a fine of not more than Five Thousand Dollars ($5,000.00), or by both such imprisonment and fine.

OREGON REVISED STATUTES

TITLE 16 CRIMES AND PUNISHMENTS
CHAPTER 164. OFFENSES AGAINST PROPERTY
CRIMINAL MISCHIEF AND RELATED OFFENSES

164.377. Computer crime.

(1) As used in this section:

(a) To "access" means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

(b) "Computer" means, but is not limited to, an electronic device which performs logical, arithmetic or memory functions by the manipulations of electronic, magnetic or optical signals or impulses, and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

(c) "Computer network" means, but is not limited to, the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals or a complex consisting of two or more interconnected computers.

(d) "Computer program" means, but is not limited to, a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from or usage of such computer system.

(e) "Computer software" means, but is not limited to, computer programs, procedures and associated documentation concerned with the operation of a computer system.

(f) "Computer system" means, but is not limited to, a set of related, connected or unconnected, computer equipment, devices and software. "Computer system" also includes any computer, device or software owned or operated by the Oregon State Lottery or rented, owned or operated by another person or entity under contract to or at the direction of the Oregon State Lottery.

(g) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. "Data" maybe in any form, in storage media,

or as stored in the memory of the computer, or in transit, or presented on a display device. "Data" includes, but is not limited to, computer or human readable forms of numbers, text, stored voice, graphics and images.

(h) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either computer or human readable form, intellectual property and any other tangible or intangible item of value.

(i) "Proprietary information" includes any scientific, technical or commercial information including any design, process, procedure, list of customers, list of suppliers, customers' records or business code or improvement thereof that is known only to limited individuals within an organization and is used in a business that the organization conducts. The information must have actual or potential commercial value and give the user of the information an opportunity to obtain a business advantage over competitors who do not know or use the information.

(j) "Services" include, but are not limited to, computer time, data processing and storage functions.

(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

(a) Devising or executing any scheme or artifice to defraud;

(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

(c) Committing theft, including, but not limited to, theft of proprietary information.

(3) Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network,

commits computer crime.

(5) (a) A violation of the provisions of subsection (2) or (3) of this section shall be a Class C felony. Except as provided in paragraph (b) of this subsection, a violation of the provisions of subsection (4) of this section shall be a Class A misdemeanor.

(b) Any violation of this section relating to a computer, computer network, computer program, computer software, computer system or data owned or operated by the Oregon State Lottery or rented, owned or operated by another person or entity under contract to or at the direction of the Oregon State Lottery Commission shall be a Class C felony.

PENNSYLVANIA CONSOLIDATED STATUTES

ANNOTATED

TITLE 18. CRIMES AND OFFENSES
PART II. DEFINITION OF SPECIFIC OFFENSES
ARTICLE C. OFFENSES AGAINST PROPERTY
CHAPTER 39. THEFT AND RELATED OFFENSES
SUBCHAPTER B. DEFINITION OF OFFENSES

§3933. Unlawful use of computer

(a) Offense defined.--A person commits an offense if he:

(1) accesses, alters, damages or destroys any computer, computer system, computer network, computer software, computer program or data base or any part thereof, with the intent to interrupt the normal functioning of an organization or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;

(2) intentionally and without authorization accesses, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program or computer data base or any part thereof; or

(3) intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or data base.

(b) Grading.--An offense under subsection (a)(1) is a felony of the third degree. An offense under subsection (a)(2) or (3) is a misdemeanor of the first degree.

(c) Definitions.--As used in this section the following words and phrases shall have the meanings given to them in this subsection:

"Access." To intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, computer network or data base.

"Computer." An electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system which performs logic, arithmetic or memory functions and includes all input, output, processing, storage, software or communication facilities which are connected or related to the device in a system or network.

"Computer network." The interconnection of two or more computers through the usage of satellite, microwave, line or other communication medium.

"Computer program." An ordered set of instructions or statements and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

"Computer software." A set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

"Computer system." A set of related, connected or unconnected computer equipment, devices and software.

"Data base." A representation of information, knowledge, facts, concepts or instructions which are being prepared or processed or have been prepared or processed in a formalized manner and are intended for use in a computer, computer system or computer network, including, but not limited to, computer printouts, magnetic storage media, punched cards or data stored internally in the memory of the computer.

"Financial instrument." Includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any computer system representation thereof.

"Property." Includes, but is not limited to, financial instruments, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

"Services." Includes, but is not limited to, computer time, data processing and storage functions.

SELECTED LEGISLATIVE HISTORY

Voice mailbox (VMB) is a "computer" for purposes of statute criminalizing unlawful use of computer; VMB is created by computer software, and messages are stored on computer disks. Com. v. Gerulis, 616 A.2d 686, 61 U.S.L.W. 2375, Super.1992.

Evidence, that defendant deposited and retrieved information from hospital's and private telephone message company's voice mailboxes (VMBs) without authority to do so, ousted authorized users from VMBs by altering passwords, and disrupted normal use of VMBs, supported conviction for

unlawful use of computer. Com. v. Gerulis, 616 A.2d 686, 61 U.S.L.W. 2375, Super.1992.

Finding that defendant intended to disrupt normal functioning of organizations, as required to support conviction for unlawful use of computer, was supported by evidence that, by changing access codes, defendant prevented authorized users from accessing voice mailboxes (VMBs) she used to market unlawfully obtained information. Com. v. Gerulis, 616 A.2d 686, 61 U.S.L.W. 2375, Super.1992.

Intent element of statute criminalizing unauthorized use of computer may be established by showing either that defendant intended to interrupt normal functioning of an organization or that defendant intended to defraud or deceive; intent element is disjunctive rather than conjunctive. Com. v. Gerulis, 616 A.2d 686, 61 U.S.L.W. 2375, Super.1992.

GENERAL LAWS OF RHODE ISLAND ANNOTATED,

REENACTMENT OF 1981
TITLE 11. CRIMINAL OFFENSES
CHAPTER 52. COMPUTER CRIME

11-52-1 Definitions.

As used in this chapter:

(A) "Access" means to approach, instruct, communicate with, store data in, enter data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network.

(B) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(C) "Computer system" means a set of related, connected or unconnected, computer equipment, devices and software.

(D) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(E) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(F) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

(G) "Computer program" means a series of instructions or statements or related data that, in actual or modified form, is capable of causing a computer or a computer system to perform specified functions in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems.

(H) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(I) "Data" means any representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared and are intended to be entered, processed or stored,

are being entered, processed or stored or have been entered, processed or stored in a computer, computer system or computer network.

(J) "Source document" means an original document or record which forms the basis of every electronic entry put into a computer, computer system or computer network.

11-52-2 Access to computer for fraudulent purposes.

Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network for the purpose of

(1) devising or executing any scheme or artifice to defraud,

(2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, or

(3) damaging, destroying, altering, deleting, or removing any program or data contained therein in connection with any scheme or artifice to defraud

shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-5.

11-52-3 Intentional access, alteration, damage or destruction.

Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-5.

11-52-4 Computer theft.

Whoever, intentionally and without claim of right, and with intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network with a value in excess of five hundred dollars ($500) shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-5. If the value is five hundred dollars

($500) or less, then said person shall be guilty of a misdemeanor and may be punishable by imprisonment for a term not exceeding one year, or by a fine of not more than one thousand dollars ($1,000), or both.

11-52-5 Penalties.

(A) Any person who is convicted of an offense which is classified as a felony under this chapter shall be fined not more than five thousand dollars ($5,000) or imprisoned for not more than five (5) years, or both.

(B) Any person who is convicted of an offense which is classified as a misdemeanor under this chapter shall be fined not more than five hundred dollars ($500) or imprisoned for not more than one year, or both.

11-52-6 Civil action.

Any person injured as a result of a violation of this chapter may bring a civil action against the violator for compensatory damages, punitive damages, court costs and for such other relief as the court deems appropriate including reasonable attorneys' fees.

11-52-7 Use of false information.

(A) Whoever intentionally or knowingly makes a transmission of false data for the purpose of submitting a claim for payment, or makes, presents or uses or causes to be made, presented, or used any data for the purpose of submitting a claim for payment with knowledge of its falsity and with knowledge that it will be used for such claim for payment shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-5.

(B) Whoever intentionally or knowingly

(1) makes a transmission of false data or

(2) makes, presents or uses or causes to be made, presented or used any data for any other purpose with knowledge of its falsity shall be guilty of a misdemeanor and shall be subject to the penalties set forth in § 11-52-5.

11-52-8 Tampering with computer source documents.

(A) Whoever intentionally or knowingly, conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source document used for a computer, computer program, computer system or computer network, when computer source document is required to be kept by law, shall be guilty of a misdemeanor and shall be subject to the provisions of § 11-52-5.

(B) Whoever intentionally or knowingly conceals, destroys, or alters or intentionally, knowingly conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source document used for a computer, computer program, computer system or computer network, when computer source document is required to be kept by law, with the intent to obstruct an official investigation by any state agency authorized by law to conduct any civil or criminal investigation, shall be guilty of a felony and shall be subject to the provisions of § 11-52-5.

CODE OF LAWS OF SOUTH CAROLINA

1976 ANNOTATED
TITLE 16. CRIMES AND OFFENSES
CHAPTER 16. COMPUTER CRIME ACT

§16-16-10. Definitions.

For purposes of this chapter:

(a) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, computer software, and communication facilities that are connected or related to a computer in a computer system or computer network but does not include any computer or other electronic device designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer.

(b) "Computer network" means the interconnection of communications lines, or any other communications facilities, with a computer through remote terminals, or a system consisting of two or more interconnected computers.

(c) "Computer program" means a series of instructions or statements executable on a computer which directs the computer system in a manner to process data or perform other specified functions.

(d) "Computer software" means a set of computer programs, data, procedures, or associated documentation concerned with the operation of a computer system.

(e) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or software.

(f) "Property" means and includes, but is not limited to, financial instruments, data, computer software, documents associated with computer systems, and computer software, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(g) "Services" means and includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data obtained within a computer system, or data contained within a computer network.

(h) "Data" means a representation of information, knowledge, facts, concepts, or instructions that has

been prepared or is being prepared in a formalized manner and has been processed, is being processed, or is intended to be processed in a computer, computer system, or computer network. Data may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or as stored in the memory of the computer or in transit or displayed on a video device.

(i) "Access" means to instruct, communicate with, attempt to communicate with, store data in, retrieve data from, or otherwise make use of or attempt to make use of any resources of a computer, computer system, or computer network.

(j) "Computer hacking" means accessing all or part of a computer, computer system, or a computer network for the purpose of establishing contact only without the intent to defraud or commit any other crime after such contact is established and without the use of computer-related services except such services as may be incidental to establishing contact.

NOTES

Computer programs as property subject to theft. 18 ALR3d 1121.
Computer as nuisance. 45 ALR4th 1212.

§16-16-20. Offenses; penalties.

(1) It is unlawful for any person to wilfully, knowingly, maliciously, and without authorization or for an unauthorized purpose to do any of the following:

(a) Directly or indirectly access or cause to be accessed any computer, computer system, or computer network for the purpose of

(i) devising or executing any scheme or artifice to defraud, or

(ii) obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises, or

(iii) committing any other crime.

(b) Alter, damage, destroy, or modify any computer, computer system, computer network, computer software, computer program, or data contained in such computer, computer

system, computer program, or computer network.

(2) A person is guilty of computer crime in the first degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim exceeds twenty-five thousand dollars. Computer crime in the first degree is a felony and, upon conviction thereof, a person must be punished by a fine of not more than one hundred twenty-five thousand dollars or imprisonment for not more than ten years, or both.

(3) (a) A person is guilty of computer crime in the second degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is greater than one thousand dollars but not more than twenty-five thousand dollars.

(b) A person is also guilty of computer crime in the second degree where

(i) he interferes with, causes to be interfered with, denies or causes to be denied any computer service to any authorized user of such computer service for the purpose of devising or executing any scheme or artifice to defraud, or obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, or committing any other felony;

(ii) he deprives the owner of possession of, or takes, transfers, conceals, or retains possession of any computer, data, computer property, or computer- related property, including all parts of a computer, computer system, computer network, computer software, computer services, or information associated with a computer, whether in a tangible or intangible form; or

(iii) the gain derived from the offense made unlawful by subsection (1) or loss suffered by the victim cannot reasonably be ascertained.

(c) Computer crime in the second degree is a felony and, upon conviction thereof, for a first offense, a person must be punished by a fine of not more than fifty thousand dollars or imprisonment for not more than three years, or both. Upon conviction for a second or subsequent offense, a person must be punished by a fine of not more than fifty thousand dollars or imprisonment for not more than seven years, or both.

(4) A person is guilty of computer crime in the third degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered

by the victim does not exceed one thousand dollars. A person is also guilty of computer crime in the third degree if he wilfully, knowingly, and without authorization or for an unauthorized purpose engages in computer hacking. Computer crime in the third degree is a misdemeanor and, upon conviction thereof, for a first offense, a person must be punished by a fine of not more than two hundred dollars or imprisonment for not more than thirty days. Upon conviction for a second or subsequent offense, a person must be punished by a fine of not more than two thousand dollars or imprisonment for not more than two years, or both.

§16-16-30. Venue.

For the purpose of venue under this chapter, any violation of this chapter shall be considered to have been committed in the county in which the violation took place; provided, that upon proper motion and the proper showing before a judge, venue may be transferred if justice would be better served by such transfer, to one of the following:

(1) In any county in which any act was performed in furtherance of any transaction which violated this chapter;

(2) In the county of the principal place of business in this State of the owner or lessee of a computer, computer system, computer network, or any part thereof which has been subject to the violation; or

(3) Any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, or other material or objects which were used in the furtherance of the violation.

§16-16-40. Applicability of other criminal law provisions.

The provisions of this chapter must not be construed to preclude the applicability of any other provision of the criminal law of this State, which presently applies or may in the future apply, to any transaction which violates this chapter.

SOUTH DAKOTA CODIFIED LAWS

TITLE 43. PROPERTY

CHAPTER 43-43B. COMPUTER PROGRAMS

43-43B-1 Unlawful uses of computer.

A person is guilty of unlawful use of a computer if he:

(1) Knowingly obtains the use of, or accesses, a computer system, or any part thereof, without the consent of the owner;

(2) Knowingly alters or destroys computer programs or data without the consent of the owner; or

(3) Knowingly obtains use of, alters, accesses or destroys a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of a computer system or any third party; or

(4) Knowingly uses or discloses to another or attempts to use or disclose to another the numbers, codes, passwords or other means of access to a computer, computer program or computer system without the consent of the owner.

43-43B-3 Obtaining use, altering or destroying system, access and disclosure without consent -- Value one thousand dollars or less.

A person convicted of a violation of subdivision 43-43B-1 (1), (2), or (4) where the value of the use, alteration, destruction, access or disclosure is one thousand dollars or less is guilty of a Class 1 misdemeanor.

43-43B-4 Obtaining use, altering or destroying system, access and disclosure without consent -- Value more than one thousand dollars.

A person convicted of a violation of subdivision 43-43B-1 (1), (2), or (4) where the value of the use, alteration, destruction, access or disclosure is more than one thousand dollars is guilty of a Class 6 felony.

SOUTH DAKOTA CODIFIED LAWS

TITLE 23A. CRIMINAL PROCEDURE
CHAPTER 23A-35A.
INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS

23A-35A-2 Offenses for which order of interception of communications may be granted.

Orders authorizing or approving the interception of wire or oral communications may be granted, subject to the provisions of this chapter when the interception may provide or has provided evidence of the commission of, or of any conspiracy to commit, the following offenses as otherwise defined by the laws of this state: murder; kidnapping; gambling; robbery; bribery; theft; unlawful use of a computer; unauthorized manufacturing, distribution or counterfeiting of controlled substances or marijuana; and, rape.
Source: SL 1969, ch 158, § 6; SDCL Supp, § 23-13A-3; SL 1980, ch 181, § 2; 1981, ch 177, § 3; 1984, ch 183.

NOTES

This chapter is not unconstitutional on grounds that it is less restrictive than federal law governing the interception of communications, 18 U.S.C. § 2510, because the state court must look to determine if the state complied with the federal statute; compliance must be had with whichever law is more constricting, be it federal or state. State v. O'Conner (1985) 378 NW 2d 248, affirmed (1987) 408 NW 2d 754.

Tape recording of drug transaction between defendant and police undercover agent made by undercover agent without knowledge of defendant was admissible at defendant's trial for distribution of marijuana even though only one party to transaction consented to recording and there was no court order authorizing recording. State v. Woods (1985) 361 NW 2d 620.

TENNESSEE CODE ANNOTATED

TITLE 39 CRIMINAL OFFENSES
CHAPTER 3 OFFENSES AGAINST PROPERTY
Part 14-- Computer Crimes

[Computer Crimes Statute Repealed]

TENNESSEE CODE ANNOTATED

TITLE 40 CRIMINAL PROCEDURE
CHAPTER 3 METHODS OF PROSECUTION
Part 2-- Fraud and Economic Crimes Prosecution

40-3-204 Fees in criminal prosecutions.

In criminal prosecutions, judges shall order that fees, in accordance with the below listed schedule, shall be paid by the person or corporations that the costs are taxed against and the clerk of the court shall collect such fees when the costs are paid. The state of Tennessee, and any county or political subdivision, shall be exempt from such costs.

. . .

(3) Other Prosecutions. In all embezzlement, fraudulent appropriation of money or property, larceny by trick, larceny after trust, false pretense or violations of the Computer Crimes Act, compiled in title 39, chapter 3, part 14 [repealed], cases, a set fee of seventy-five dollars ($75.00) shall be paid regardless of the amount alleged to have been stolen or taken.

TENNESSEE CODE ANNOTATED

TITLE 40 CRIMINAL PROCEDURE
CHAPTER 35 CRIMINAL SENTENCING REFORM ACT OF 1989
Part 1-- General Provisions

40-35-118 Classification of prior felony offenses.

For the purpose of determining the classification of felony offenses in title 39 committed prior to November 1, 1989, the following classifications shall be used:

Code	Offense	Class
	. . .	
39-3-1404(b)	Intentionally damaging or destroying computer system	D
39-3-1404(c)	Concealing proceeds of computer crime	D
39-3-1404(a)	Willfully gaining access to computer system with intent to defraud	E

TENNESSEE CODE ANNOTATED

TITLE 39 CRIMINAL OFFENSES
CHAPTER 14 OFFENSES AGAINST PROPERTY
Part 6-- Computer Offenses

39-14-601 Definitions for computer offenses.

The following definitions apply in this part, unless the context otherwise requires:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of a computer, computer system or computer network;

(2) "Computer" means a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job;

(3) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them;

(4) "Computer program" means an ordered set of data that are coded instructions or statements that, when executed by a computer, cause the computer to process data;

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system or computer network;

(6) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one (1) or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(7) "Data" is a representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared in a formalized manner, and is intended to be stored or processed, or is being stored or processed, or has been stored or processed, in a computer, computer system or computer network;

(8) "Financial instrument" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, marketable security, or any computer system representation thereof;

(9) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(10) "To process" is to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(11) "Property" includes, but is not limited to, intellectual property, financial instruments, data, computer programs, documentation associated with data, computers, computer systems and computer programs, all in machine-readable or human-readable form, and any tangible or intangible item of value; and

(12) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer program or data to perform tasks.

39-14-602 Violations -- Penalties.

(a) Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of obtaining money, property, or services for himself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection and is subject to the penalties of § 39-14-105.

(b) Whoever intentionally and without authorization, directly or indirectly:

(1) Accesses; or

(2) Alters, damages, destroys, or attempts to damage or destroy, any computer, computer system, computer network, computer software, program or data;

violates this subsection.

(c) A violation of subdivision (b)(1) is a Class C misdemeanor.

(d) A violation of subdivision (b)(2) is punished as in § 39-14-105.

(e) Whoever receives, conceals, uses, or aids another in receiving, concealing or using any proceeds

resulting from a violation of either subsection (a) or subdivision (b)(2), knowing the same to be proceeds of such violation, or whoever receives, conceals, uses, or aids another in receiving, concealing or using, any books, records, documents, property, financial instrument, computer software, program, or other material, property, or objects, knowing the same to have been used in violating either subsection (a) or subdivision (b)(2) violates this subsection and is subject to the penalties of § 39-14-105.

39-14-603 Venue.

For the purposes of venue under the provisions of this part, any violation of this part shall be considered to have been committed:

(1) In any county in which any act was performed in furtherance of any transaction violating this part;

(2) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program or other material, objects or items which were used in furtherance of the violation; and

(3) In any county from which, to which or through which any access to a computer, computer system, or computer network was made, whether by wire, electromagnetic waves, microwaves or any other means of communication.

TENNESSEE CODE ANNOTATED

TITLE 40 CRIMINAL PROCEDURE
CHAPTER 35 CRIMINAL SENTENCING REFORM ACT OF 1989
Part 1-- General Provisions

40-35-110 Classification of offenses.

(a) Felonies are classified, for the purpose of sentencing, into five (5) categories:

(1) Class A felonies;
(2) Class B felonies;
(3) Class C felonies;
(4) Class D felonies; and
(5) Class E felonies.

(b) An offense designated a felony without specification as to category is a Class E felony.

(c) Misdemeanors are classified, for the purpose of sentencing, into three (3) categories:

(1) Class A misdemeanors;
(2) Class B misdemeanors; and
(3) Class C misdemeanors.

(d) An offense designated as a misdemeanor without specification as to category is a Class A misdemeanor.

The following table shows the classification of felony and misdemeanor offenses in title 39. For first degree murder, see § 39-11-117.

CLASSIFICATION OF THE REVISED CRIMINAL CODE

Class B Felonies

. . .

39-14-602 Alters, damages, or attempts to damage or destroy any computer, computer system or computer network or computer program or data ($60,000 or more)

Class C Felonies

. . .

39-14-602 Alters, damages, or attempts to damage or destroy any computer, computer system or

computer network or computer program or data ($10,000-$59,999)

Class D Felonies

. . .

39-14-602 Alters, damages or attempts to damage or destroy any computer, computer system or computer network or computer program or data ($1,000-$9,999)

Class E Felonies

. . .

39-14-602 Alters, damages, or attempts to damage or destroy any computer, program or data ($501-$999)

Class A Misdemeanors

. . .

39-14-602 Alters, damages, or attempts to damage or destroy a computer, computer system or computer network or computer software program or data (up to $500)

Class C Misdemeanors

. . .

39-14-602(b)(1) Accessing computer

TEXAS STATUTES AND CODES ANNOTATED

PENAL CODE
TITLE 7. OFFENSES AGAINST PROPERTY
CHAPTER 33. COMPUTER CRIMES

§33.01. Definitions

In this chapter:

(1) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(2) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(3) "Computer network" means the interconnection of two or more computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(4) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(5) "Computer security system" means the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(6) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(7) "Computer system" means any combination of a computer or computers with the documentation, computer software, or physical facilities supporting the computer.

(8) "Computer software" means a set of computer programs, procedures, and associated

documentation related to the operation of a computer, computer system, or computer network.

(9) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself and to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(10) "Damage" includes partial or total alteration, damage, or erasure of stored data, or interruption of computer services.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, and punchcards, or may be stored internally in the memory of the computer.

(12) "Electric utility" has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).

§33.02. Breach of Computer Security

(a) A person commits an offense if the person:

(1) uses a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer and the actor knows that there exists a computer security system intended to prevent him from making that use of the computer; or

(2) gains access to data stored or maintained by a computer without the effective consent of the owner or licensee of the data and the actor knows that there exists a computer security system intended to prevent him from gaining access to that data.

(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict the use of a computer or to restrict access to data stored or maintained by a computer.

(c) An offense under this section is a Class A misdemeanor.

§33.03. Harmful Access

(a) A person commits an offense if the person intentionally or knowingly and without authorization from the owner of the computer or a person authorized to license access to the computer:

(1) damages, alters, or destroys a computer, computer program or software, computer system, data, or computer network;

(2) causes a computer to interrupt or impair a government operation, public communication, public transportation, or public service providing water or gas;

(3) uses a computer to:

(A) tamper with government, medical, or educational records; or

(B) receive or use records that were not intended for public dissemination to gain an advantage over business competitors;

(4) obtains information from or introduces false information into a computer system to damage or enhance the data or credit records of a person;

(5) causes a computer to remove, alter, erase, or copy a negotiable instrument; or

(6) inserts or introduces a computer virus into a computer program, computer network, or computer system.

(b) An offense under this section is a:

(1) felony of the second degree if the value of the loss or damage caused by the conduct is $20,000 or more;

(2) felony of the third degree if the value of the loss or damage caused by the conduct is $750 or more but less than $20,000; or

(3) Class A misdemeanor if the value of the loss or damage caused by the conduct is $200 or

more but less than $750.

NOTES

This section did not cover speech or conduct protected by First Amendment and was not unconstitutionally overbroad. Burleson v. State (App. 2 Dist.1991) 802 S.W.2d 429, review refused.

This section was not unconstitutionally vague as applied to defendant who allegedly deleted data from his employer's computer system; although defendant claimed that statute could be applied to persons who act negligently, defendant was charged with acting knowingly and intentionally. Burleson v. State (App. 2 Dist.1991) 802 S.W.2d 429, review refused.

Evidence in prosecution for harmful access to computer was sufficient to establish that records in employer's computer system were deleted, as alleged in indictment; evidence indicated that, although records were not physically deleted or destroyed, they were logically deleted so that they were inaccessible to computer for processing employer's payroll commission file. Burleson v. State (App. 2 Dist.1991) 802 S.W.2d 429, review refused.

Evidence in prosecution for harmful access to computer was sufficient to support finding that data was deleted from "computer memory and computer storage", as alleged in indictment; evidence indicated that records were deleted from input, processing, or storage connected or related to computer's central processing unit. Burleson v. State (App. 2 Dist.1991) 802 S.W.2d 429, review refused.

Evidence in prosecution for harmful access to the computer was sufficient to establish that computer malfunctioned, as alleged in indictment; evidence indicated that computer shut down for a number of hours because defendant booby-trapped computer with a program. Burleson v. State (App. 2 Dist.1991) 802 S.W.2d 429, review refused.

§33.04. Defenses

It is an affirmative defense to prosecution under Sections 33.02 and 33.03 of this code that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

§33.05. Assistance by Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

TEXAS STATUTES AND CODES ANNOTATED

CODE OF CRIMINAL PROCEDURE
PART I--CODE OF CRIMINAL PROCEDURE OF 1965
LIMITATION AND VENUE
CHAPTER THIRTEEN--VENUE

Art. 13.25. Computer crimes

(a) In this section "computer," "computer network," "computer program," and "computer system" have the meanings assigned to those terms in Section 33.01, Penal Code.

(b) An offense under Chapter 33, Penal Code, may be prosecuted in:

(1) the county of the principal place of business of the owner or lessee of a computer, computer system, or computer network involved in the violation;

(2) any county in which a defendant had control or possession of any proceeds from the violation or any books, records, documents, property, negotiable instruments, computer programs, or other material that were used in furtherance of the violation; or

(3) any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

UTAH CODE, 1953

TITLE 76. CRIMINAL CODE
CHAPTER 6. OFFENSES AGAINST PROPERTY
PART 7. COMPUTER CRIMES

76-6-701 Computer Crimes Act -- Short title.

This part is known as the "Utah Computer Crimes Act."

76-6-702 Computer Crimes Act -- Definitions.

As used in this part:

(1) "Access" means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

(2) "Computer" means any electronic device or communication facility with data processing ability.

(3) "Computer system" means a set of related, connected or unconnected, devices, software, or other related computer equipment.

(4) "Computer network" means the interconnection of communication or telecommunication lines between computers or computers and remote terminals.

(5) "Computer property" includes, but is not limited to, electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

(6) "Services" include, but are not limited to, computer time, data manipulation, and storage functions.

(7) "Financial instrument" includes, but is not limited to, any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(8) "Software" or "program" means a series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results including, but not limited to, system control programs, application programs, or copies of any of them.

76-6-703 Computer crimes and penalties.

(1) A person who gains or attempts to gain access to and without authorization intentionally, and to the damage of another, alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, program, or software is guilty of a felony of the third degree.

(2) A person who intentionally and without authorization uses a computer, computer network, computer property, or computer system to gain or attempt to gain access to any other computer, computer network, computer property, or computer system, program, or software, to the damage of another, and alters, damages, destroys, discloses, or modifies any of these, is guilty of a felony of the third degree.

(3) A person who uses or knowingly allows another person to use any computer, computer network, computer property, or computer system, program, or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations, is guilty of a felony of the second degree.

(4) A person who intentionally, and without authorization, interferes with or interrupts computer services to another authorized to receive the services is guilty of a class A misdemeanor.

(5) A person who intentionally and without authorization damages or destroys, in whole or in part, any computer, computer network, computer property, or computer system is guilty of a class A misdemeanor unless the amount of damage exceeds $1,000, in which case the person is guilty of a felony of the third degree.

76-6-704 Computer Crimes Act -- Attorney general, county attorney, or district attorney to prosecute -- Conduct violating other statutes.

(1) The attorney general, district attorney, or the county attorney shall prosecute suspected criminal violations of this part.

(2) Prosecution under this part does not prevent any prosecutions under any other law.

76-6-705 Reporting violations.

Every person, except those to whom a statutory or common law privilege applies, who has reason to believe that the provisions of Section 76-6-703 are being or have been violated shall report the suspected violation to the attorney general, or county attorney, or, if within a prosecution district, the district attorney of the county or prosecution district in which part or all of the violations occurred.

CODE OF VIRGINIA

TITLE 8.01. CIVIL REMEDIES AND PROCEDURE
CHAPTER 3. ACTIONS.
ARTICLE 3. INJURY TO PERSON OR PROPERTY

§8.01-40.1 Action for injury resulting from violation of Computer Crimes Act; limitations.

Any person whose property or person is injured by reason of a violation of the provisions of the Virginia Computer Crimes Act (§ 18.2-152.1 et seq.) may sue and recover damages as provided in § 18.2-152.12. An action shall be commenced before the earlier of

(i) five years after the last act in the course of conduct constituting a violation of the Computer Crimes Act or

(ii) two years after the plaintiff discovers or reasonably should have discovered the last act in the course of conduct constituting a violation of the Computer Crimes Act.

CODE OF VIRGINIA

TITLE 18.2. CRIMES AND OFFENSES GENERALLY
CHAPTER 5. CRIMES AGAINST PROPERTY.
ARTICLE 7.1. COMPUTER CRIMES.

§18.2-152.1 Short title.

This article shall be known and may be cited as the "Virginia Computer Crimes Act."

§18.2-152.2 Definitions.

For purposes of this article:

"Computer" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

"Computer data" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

"Computer network" means a set of related, remotely connected devices and any communications facilities including more than one computer with the capability to transmit data among them through the communications facilities.

"Computer operation" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

"Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer

operations.

"Computer services" includes computer time or services or data processing services or information or data stored in connection therewith.

"Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

"Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

"Owner" means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

"Person" shall include any individual, partnership, association, corporation or joint venture.

"Property" shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
   a. Tangible or intangible;
   b. In a format readable by humans or by a computer;
   c. In transit between computers or within a computer network or between any devices which comprise a computer; or
   d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person "uses" a computer or computer network when he:

1. Attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;

2. Attempts to cause or causes the withholding or denial of the use of a computer,

computer network, computer program, computer data or computer software to another user; or

3. Attempts to cause or causes another person to put false information into a computer.

A person is "without authority" when he has no right or permission of the owner to use a computer, or, he uses a computer in a manner exceeding such right or permission.

§18.2-152.3 Computer fraud.

Any person who uses a computer or computer network without authority and with the intent to:

1. Obtain property or services by false pretenses;

2. Embezzle or commit larceny; or

3. Convert the property of another shall be guilty of the crime of computer fraud. If the value of the property or services obtained is $200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than $200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.

§18.2-152.4 Computer trespass; penalty.

Any person who uses a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove computer data, computer programs, or computer software from a computer or computer network;

2. Cause a computer to malfunction regardless of how long the malfunction persists;

3. Alter or erase any computer data, computer programs, or computer software;

4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;

5. Cause physical injury to the property of another; or

6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network shall be guilty of the crime of computer trespass, which shall be punishable as a Class 1 misdemeanor. If such act is done maliciously and the value of the property damaged is $2,500 or more, the offense shall be punishable as a Class 6 felony.

§18.2-152.5 Computer invasion of privacy.

A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

B. The crime of computer invasion of privacy shall be punishable as a Class 3 misdemeanor.

§18.2-152.6 Theft of computer services.

Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor.

§18.2-152.7 Personal trespass by computer.

A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.

B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act be done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 1 misdemeanor.

§18.2-152.8 Property capable of embezzlement.

For purposes of §18.2-111, personal property subject to embezzlement shall include:

1. Computers and computer networks;

2. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:

    a. Tangible or intangible;

    b. In a format readable by humans or by a computer;

    c. In transit between computers or within a computer network or between any devices which comprise a computer; or

    d. Located on any paper or in any device on which it is stored by a computer or by a human; and

3. Computer services.

§18.2-152.9 Limitation of prosecution.

Notwithstanding the provisions of §19.2-8, prosecution of a crime which is punishable as a misdemeanor pursuant to this article must be commenced before the earlier of

(i) five years after the commission of the last act in the course of conduct constituting a violation of this article or

(ii) one year after the existence of the illegal act and the identity of the offender are discovered by the Commonwealth, by the owner, or by anyone else who is damaged by such violation.

§18.2-152.10 Venue for prosecution.

For the purpose of venue under this article, any violation of this article shall be considered to have been

committed in any county or city:

1. In which any act was performed in furtherance of any course of conduct which violated this article;

2. In which the owner has his principal place of business in the Commonwealth;

3. In which any offender had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, computer data, or other material or objects which were used in furtherance of the violation;

4. From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;

5. In which the offender resides; or

6. In which any computer which is an object or an instrument of the violation is located at the time of the alleged offense.

§18.2-152.11 Article not exclusive.

The provisions of this article shall not be construed to preclude the applicability of any other provision of the criminal law of this Commonwealth which presently applies or may in the future apply to any transaction or course of conduct which violates this article, unless such provision is clearly inconsistent with the terms of this article.

§18.2-152.12 Civil relief; damages.

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the

computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

C. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

D. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1.

§18.2-152.13 Severability.

If any provision or clause of this article or application thereof to any person or circumstances is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are declared to be severable.

§18.2-152.14 Computer as instrument of forgery.

The creation, alteration, or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under Article 1 (s 18.2-168 et seq.) of Chapter 6 of this Title, will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in Article 1 (s 18.2-168 et seq.) of Chapter 6 of this Title if a creation, alteration, or deletion of computer data was involved in lieu of a tangible document or instrument.

CODE OF WASHINGTON ANNOTATED

TITLE 9A. WASHINGTON CRIMINAL CODE
CHAPTER 9A.52--BURGLARY AND TRESPASS

9A.52.110. Computer trespass in the first degree

(1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another; and

(a) The access is made with the intent to commit another crime; or

(b) The violation involves a computer or data base maintained by a government agency.

(2) Computer trespass in the first degree is a class C felony.

SELECTED LEGISLATIVE HISTORY

Evidence showed at most unauthorized use of computer data, which was not prohibited by this section, and was insufficient to sustain conviction for computer trespass; defendant, a university police officer who had an access code and permission to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of computer, was found retrieving computer printouts of college coeds which were in no way connected to any ongoing police investigation. State v. Olson (1987) 47 Wash.App. 514, 735 P.2d 1362.

Trial court was required to find lack of authorization to use computer beyond a reasonable doubt after independently reviewing evidence in prosecution for computer trespass, and it committed error when it relied on pretrial order to find lack of authority to access computer. State v. Olson (1987) 47 Wash.App. 514, 735 P.2d 1362.

9A.52.130. Computer trespass--Commission of other crime

A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.

WEST VIRGINIA CODE 1966

CHAPTER 61. CRIMES AND THEIR PUNISHMENT

ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT

§61-3C-1 Short title.

This act shall be known and may be cited as the "West Virginia Computer Crime and Abuse Act."

§61-3C-2 Legislative findings.

The Legislature finds that:

(a) The computer and related industries play an essential role in the commerce and welfare of this state.

(b) Computer-related crime is a growing problem in business and government.

(c) Computer-related crime has a direct effect on state commerce and can result in serious economic and, in some cases, physical harm to the public.

(d) Because of the pervasiveness of computers in today's society, opportunities are great for computer related crimes through the introduction of false records into a computer or computer system, the unauthorized use of computers and computer facilities, the alteration and destruction of computers, computer programs and computer data, and the theft of computer resources, computer software and computer data.

(e) Because computers have now become an integral part of society, the Legislature recognizes the need to protect the rights of owners and legitimate users of computers and computer systems, as well as the privacy interest of the general public, from those who abuse computers and computer systems.

(f) While various forms of computer crime or abuse might possibly be the subject of criminal charges or civil suit based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which specifically proscribes various forms of computer crime and abuse and provides criminal penalties and civil remedies therefor.

§61-3C-3 Definitions.

As used in this article, unless the context clearly indicates otherwise:

(a) "Access" means to instruct, communicate with, store data in, retrieve data from, intercept data from, or otherwise make use of any computer, computer network, computer program, computer software, computer data or other computer resources.

(b) "Authorization" means the express or implied consent given by a person to another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number.

(c) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithematic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device. The term "computer" includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator or other similar device.

(d) "Computer data" means any representation of knowledge, facts, concepts, instruction, or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer network, computer program or computer software, and may be in any medium, including, but not limited to, computer printouts, microfilm, microfiche, magnetic storage media, optical storage media, punch paper tape or punch cards, or it may be stored internally in read-only memory or random access memory of a computer or any other peripheral device.

(e) "Computer network" means a set of connected devices and communication facilities, including more than one computer, with the capability to transmit computer data among them through such communication facilities.

(f) "Computer operations" means arithmetic, logical, storage, display, monitoring or retrieval functions or any combination thereof, and includes, but is not limited to, communication with, storage of data in or to, or retrieval of data from any device and the human manual manipulation of electronic magnetic impulses. A "computer operation" for a particular computer shall also mean any function for which that computer was designed.

(g) "Computer program" means an ordered set of computer data representing instructions or statements, in a form readable by a computer, which controls, directs, or otherwise influences the functioning of a computer or computer network.

(h) "Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

(i) "Computer services" means computer access time, computer data processing, or computer data storage, and the computer data processed or stored in connection therewith.

(j) "Computer supplies" means punchcards, paper tape, magnetic tape, magnetic disks or diskettes, optical disks or diskettes, disk or diskette packs, paper, microfilm, and any other tangible input, output or storage medium used in connection with a computer, computer network, computer data, computer software or computer program.

(k) "Computer resources" includes, but is not limited to, information retrieval; computer data processing, transmission and storage; and any other functions performed, in whole or in part, by the use of a computer, computer network, computer software, or computer program.

(lx) "Owner" means any person who owns or leases or is a licensee of a computer, computer network, computer data, computer program, computer software, computer resources or computer supplies.

(m) "Person" means any natural person, general partnership, limited partnership, trust, association, corporation, joint venture, or any state, county or municipal government and any subdivision, branch, department or agency thereof.

(n) "Property" includes:

(1) Real property;

(2) Computers and computer networks;

(3) Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:

(i) Tangible or intangible;

(ii) In a format readable by humans or by a computer;

(iii) In transit between computers or within a computer network or between any devices which comprise a computer; or

(iv) Located on any paper or in any device on which it is stored by a computer or by a human; and

(4) Computer services.

(o) "Value" means having any potential to provide any direct or indirect gain or advantage to any person.

(p) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any computerized representation thereof.

(q) "Value of property or computer services" shall be

(1) the market value of the property or computer services at the time of a violation of this article; or

(2) if the property or computer services are unrecoverable, damaged, or destroyed as a result of a violation of section three or four [§ 61-3C-3 or § 61-3C-4] of this article, the cost of reproducing or replacing the property or computer services at the time of the violation.

§61-3C-4 Computer fraud; penalties.

Any person who, knowingly and willfully, directly or indirectly, accesses or causes to be accessed any computer, computer services or computer network for the purpose of

(1) executing any scheme or artifice to defraud or

(2) obtaining money, property or services by means of fraudulent pretenses, representations or promises shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

§61-3C-5 Unauthorized access to computer services.

Any person who knowingly, willfully and without authorization, directly or indirectly, accesses or causes

to be accessed a computer or computer network with the intent to obtain computer services shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred dollars nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-6 Unauthorized possession of computer data or programs.

(a) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of five thousand dollars or more shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

(b) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of less than five thousand dollars shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county jail for not more than one year, or both.

§61-3C-7 Alteration, destruction, etc., of computer equipment.

Any person who knowingly, willfully and without authorization, directly or indirectly, tampers with, deletes, alters, damages or destroys or attempts to tamper with, delete, alter, damage or destroy any computer, computer network, computer software, computer resources, computer program or computer data shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or confined in the penitentiary not more than ten years, or both, or, in the discretion of the court, be fined not less than two hundred nor more than one thousand dollars and confined in the county jail not more than one year.

§61-3C-8 Disruption of computer services.

Any person who knowingly, willfully and without authorization, directly or indirectly, disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized recipient or user of such computer services, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-9 Unauthorized possession of computer information, etc.

Any person who knowingly, willfully and without authorization possesses any computer data, computer software, computer supplies or a computer program which he knows or reasonably should know was obtained in violation of any section of this article shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail for not more than one year, or both.

§61-3C-10 Disclosure of computer security information.

Any person who knowingly, willfully and without authorization discloses a password, identifying code, personal identification number or other confidential information about a computer security system to another person shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail for not more than six months, or both.

§61-3C-11 Obtaining confidential public information.

Any person who knowingly, willfully and without authorization accesses or causes to be accessed any computer or computer network and thereby obtains information filed by any person with the state or any county or municipality which is required by law to be kept confidential shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail not more than six months, or both.

§61-3C-12 Computer invasion of privacy.

Any person who knowingly, willfully and without authorization accesses a computer or computer network and examines any employment, salary, credit or any other financial or personal information relating to any other person, after the time at which the offender knows or reasonably should know that he is without authorization to view the information displayed, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail for not more than six months, or both.

§61-3C-13 Fraud and related activity in connection with access devices.

(a) As used in this section, the following terms shall have the following meanings:

(1) "Access device" means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) "Counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) "Unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained without authority;

(4) "Produce" includes design, alter, authenticate, duplicate, or assemble;

(5) "Traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.

(b) Any person who knowingly and willfully possesses any counterfeit or unauthorized access device shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county jail for not more than six months, or both.

(c) Any person who knowingly, willfully and with intent to defraud possesses a counterfeit or unauthorized access device or who knowingly, willfully and with intent to defraud, uses, produces or traffics in any counterfeit or unauthorized access device shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

(d) This section shall not prohibit any lawfully authorized investigative or protective activity of any state, county or municipal law-enforcement agency.

§61-3C-14 Endangering public safety.

Any person who accesses a computer or computer network and knowingly, willfully and without authorization

(a) interrupts or impairs the providing of services by any private or public utility;

(b) interrupts or impairs the providing of any medical services;

(c) interrupts or impairs the providing of services by any state, county or local government agency, public carrier or public communication service; or otherwise endangers public safety

shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than fifty thousand dollars or imprisoned not more than twenty years, or both.

§61-3C-15 Computer as instrument of forgery.

The creation, alteration or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under section five [§ 61-4-5], article four, chapter sixty-one of this code will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in section five, article four, chapter sixty-one if a creation, alteration or deletion of computer data was involved in lieu of a tangible document or instrument.

§61-3C-16 Civil relief; damages.

(a) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor in circuit court and may be entitled to recover for each violation:

(1) Compensatory damages;

(2) Punitive damages; and

(3) Such other relief, including injunctive relief, as the court may deem appropriate.

Without limiting the generality of the term, "damages" shall include loss of profits.

(b) At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a manner as to protect the secrecy and security of the computer network, computer data, computer program or computer software involved in order to prevent any possible recurrence of the same or a similar act by another person or to protect any trade secret or confidential information of any person. For the purposes of this section "trade secret" means the whole or any portion or phase of any scientific or technological information, design, process, procedure or formula or improvement which is secret and of value.

A trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those authorized by the owner to have access thereto for a limited purpose.

(c) The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(d) A civil action under this section must be commenced before the earlier of:

(1) Five years after the last act in the course of conduct constituting a violation of this article; or

(2) two years after the plaintiff discovers or reasonably should have discovered the last act in the course of conduct constituting a violation of this article.

§61-3C-17 Defenses to criminal prosecution.

(a) In any criminal prosecution under this article, it shall be a defense that:

(1) The defendant had reasonable grounds to believe that he had authority to access or could not have reasonably known he did not have authority to access the computer, computer network, computer data, computer program or computer software in question; or

(2) The defendant had reasonable grounds to believe that he had the right to alter or destroy the computer data, computer software or computer program in question; or

(3) The defendant had reasonable grounds to believe that he had the right to copy, reproduce, duplicate or disclose the computer data, computer program, computer security system information or computer software in question.

(b) Nothing in this section shall be construed to limit any defense available to a person charged with a violation of this article.

§61-3C-18 Venue.

For the purpose of criminal and civil venue under this article, any violation of this article shall be considered

to have been committed:

(1) In any county in which any act was performed in furtherance of any course of conduct which violates this article;

(2) In the county of the principal place of business in this state of the aggrieved owner of the computer, computer data, computer program, computer software or computer network, or any part thereof;

(3) In any county in which any violator had control or possession of any proceeds of the violation or any books, records, documentation, property, financial instrument, computer data, computer software, computer program, or other material or objects which were used in furtherance of or obtained as a result of the violation;

(4) In any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves or any other means of communication; and

(5) In the county in which the aggrieved owner or the defendant resides or either of them maintains a place of business.

§61-3C-19 Prosecution under other criminal statutes not prohibited.

Criminal prosecution pursuant to this article shall not prevent prosecution pursuant to any other provision of law.

§61-3C-20 Personal jurisdiction.

Any person who violates any provision of this article and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.

§61-3C-21 Severability.

If any provision of this article or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect any other provisions or applications of this article which can be given effect without the invalid provision or application, and to that end the provisions of this article are declared to be severable.

WISCONSIN STATUTES ANNOTATED

CHAPTER 943. CRIMES AGAINST PROPERTY
MISAPPROPRIATION

943.70. Computer crimes

(1) Definitions. In this section:

(a) "Computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network.

(b) "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of 2 or more interconnected computers.

(c) "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

(d) "Computer software" means a set of computer programs, procedures or associated documentation used in the operation of a computer system.

(dm) "Computer supplies" means punchcards, paper tape, magnetic tape, disk packs, diskettes and computer output, including paper and microform.

(e) "Computer system" means a set of related computer equipment, hardware or software.

(f) "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed or is intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, punched cards and as stored in the memory of the computer. Data are property.

(g) "Financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or credit card, transaction authorization mechanism, marketable security and any computer representation of them.

(h) "Property" means anything of value, including but not limited to financial instruments, information, electronically produced data, computer software and computer programs.

(i) "Supporting documentation" means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

(2) Offenses against computer data and programs.

(a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies data, computer programs or supporting documentation.

2. Destroys data, computer programs or supporting documentation.

3. Accesses data, computer programs or supporting documentation.

4. Takes possession of data, computer programs or supporting documentation.

5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2, 3 or 4 applies.

2. A Class E felony if the offense is committed to defraud or to obtain property.

3. A Class D felony if the damage is greater than $2,500 or if it causes an interruption or impairment of governmental operations or public communication, of transportation or of a supply of water, gas or other public service.

4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(3) Offenses against computers, computer equipment or supplies.

(a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2, 3 or 4 applies.

2. A Class E felony if the offense is committed to defraud or obtain property.

3. A Class D felony if the damage to the computer, computer system, computer network, equipment or supplies is greater than $2,500.

4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(4) Computer use restriction. In addition to the other penalties provided for violation of this section, a judge may place restrictions on the offender's use of computers. The duration of any such restrictions may not exceed the maximum period for which the offender could have been imprisoned; except if the offense is punishable by forfeiture, the duration of the restrictions may not exceed 90 days.

(5) Injunctive relief. Any aggrieved party may sue for injunctive relief under ch. 813 to compel compliance with this section. In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.

NOTES

968.28. Application for court order to intercept communications

The attorney general together with the district attorney of any county may approve a request of an investigative or law enforcement officer to apply to the chief judge of the judicial administrative district for the county where the interception is to take place for an order authorizing or approving

the interception of wire, electronic or oral communications. The chief judge may under § 968.30 grant an order authorizing or approving the interception of wire, electronic or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense for which the application is made. The authorization shall be permitted only if the interception may provide or has provided evidence of the commission of the offense of homicide, felony murder, kidnapping, commercial gambling, bribery, extortion or dealing in controlled substances or a computer crime that is a felony under § 943.70 or any conspiracy to commit any of the foregoing offenses.

968.28. Application for court order to intercept communications

The attorney general together with the district attorney of any county may approve a request of an investigative or law enforcement officer to apply to the chief judge of the judicial administrative district for the county where the interception is to take place for an order authorizing or approving the interception of wire or oral communications. The chief judge may under § 968.30 grant an order authorizing or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense for which the application is made. The authorization shall be permitted only if the interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, commercial gambling, bribery, extortion or dealing in controlled substances or a computer crime which is a felony under § 943.70 or any conspiracy to commit any of the foregoing offenses.

SELECTED LEGISLATIVE HISTORY

Electronic Surveillance Control Law was not unconstitutional on theory that it was overbroad and authorized "general searches" and failed to provide for adequate notice and to require inventory of interceptions or on theory that the Act permits an officer too great an exercise of discretion as to communications intercepted or that discretion granted authorizing judge to extend order authorizing surveillance beyond 30-day limit was improper. Hussong v. State (1974) 215 N.W.2d 390, 62 Wis.2d 577.

Since interception by government agents of informant's telephone call to defendant, who during course of call agreed to sell informant narcotics, was exclusively done by federal agents and was lawful under federal law, Wisconsin law did not govern its admissibility into evidence in federal prosecution for unlawful possession and distribution of lysergic acid diethylamide, notwithstanding that telephone call may have been a privileged communication under Wisconsin law. U.S. v. Beni (D.C.1975) 397 F.Supp. 1086.

General rule is that evidence obtained by state by means of illegal electronic surveillance violates U.S.C.A. Const.Amend. 4 and must be suppressed. State v. Waste Management of Wisconsin, Inc. (1978) 261 N.W.2d 147, 81 Wis.2d 555, certiorari denied 99 S.Ct. 189, 439 U.S. 865, 58 L.Ed.2d 175.

Evidence that defendant carried grudge against murder victim and had been seen in general area of murder, that spent shells found at site of murder were identical to shells previously fired from defendant's rifle and that continual dialogue was taking place between individual and defendant concerning defendant's rifle which had not yet been recovered constituted sufficient probable cause for issuance of wiretap order under Wisconsin Electronic Surveillance Control Law. Hussong v. State (1974) 215 N.W.2d 390, 62 Wis.2d 577.

An existence of probable cause for issuance of order authorizing electronic surveillance necessitates finding that reasonable man, when faced with evidence of individual case, would believe that particular communications concerning the offense could be obtained through such surveillance. Id.

WYOMING STATUTES 1977

TITLE 6. Crimes and Offenses
CHAPTER 3. Offenses Against Property
ARTICLE 5. Computer Crimes

§6-3-501 Definitions.

(a) As used in this article:

(i) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network;

(ii) "Computer" means an internally programmed, automatic device which performs data processing;

(iii) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one (1) computer system with capability to transmit data among them through communication facilities;

(iv) "Computer program" means an ordered set of data representing coded instructions or statements which when executed by a computer cause the computer to process data;

(v) "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system;

(vi) "Computer system" means a set of related, connected or unconnected, computer equipment, devices or computer software;

(vii) "Computer system services" means providing a computer system or computer network to perform useful work;

(viii) "Financial instrument" means a check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security;

(ix) "Intellectual property" means data, including programs;

(x) "Property" includes financial instruments, information, electronically produced data, computer software and programs in machine-readable or human-readable form;

(xi) "Trade secret" means the whole or a portion or phase of a formula, pattern, device, combination of devices or compilation of information which is for use, or is used in the operation of a business and which provides the business an advantage or an opportunity to obtain an advantage over those who do not know or use it. "Trade secret" includes any scientific, technical or commercial information including any design, process, procedure, list of suppliers, list of customers, business code or improvement thereof. Irrespective of novelty, invention, patentability, the state of the prior art and the level of skill in the business, art or field to which the subject matter pertains, when the owner of a trade secret takes measures to prevent it from becoming available to persons other than those selected by the owner to have access to it for limited purposes, the trade secret is considered to be:

(A) Secret;

(B) Of value;

(C) For use or in use by the business; and

(D) Providing an advantage or an opportunity to obtain an advantage to the business over those who do not know or use it.

NOTE

There is no subsection (b) in this section as it appeared in the 1982 printed act.

§6-3-502 Crimes against intellectual property; penalties.

(a) A person commits a crime against intellectual property if he knowingly and without authorization:

(i) Modifies data, programs or supporting documentation residing or existing internal or external to a computer, computer system or computer network;

(ii) Destroys data, programs or supporting documentation residing or existing internal or external to a computer, computer system or computer network;

(iii) Discloses or takes data, programs, or supporting documentation having a value of more than seven hundred fifty dollars ($750.00) and which is a trade secret or is confidential, as provided by law, residing or existing internal or external to a computer, computer system or computer network.

(b) A crime against intellectual property is:

(i) A felony punishable by imprisonment for not more than three (3) years, a fine of not more than three thousand dollars ($3,000.00), or both, except as provided in paragraph (ii) of this subsection;

(ii) A felony punishable by imprisonment for not more than ten (10) years, a fine of not more than ten thousand dollars ($10,000.00), or both, if the crime is committed with the intention of devising or executing a scheme or artifice to defraud or to obtain property.

§6-3-503 Crimes against computer equipment or supplies; interruption or impairment of governmental operations or public services; penalties.

(a) A person commits a crime against computer equipment or supplies if he knowingly and without authorization, modifies equipment or supplies used or intended to be used in a computer, computer system or computer network. A crime against computer equipment or supplies is:

(i) A misdemeanor punishable by imprisonment for not more than six (6) months, a fine of not more than seven hundred fifty dollars ($750.00), or both, except as provided in paragraph (ii) of this subsection;

(ii) A felony punishable by imprisonment for not more than ten (10) years, a fine of not more than ten thousand dollars ($10,000.00), or both, if the crime is committed with the intention of devising or executing a scheme or artifice to defraud or to obtain property.

(b) A person who knowingly and without authorization destroys, injures or damages a computer, computer system or computer network and thereby interrupts or impairs governmental operations or public communication, transportation or supplies of water, gas or other public service, is guilty of a felony punishable by imprisonment for not more than three (3) years, a fine of not more than three thousand dollars ($3,000.00), or both.

§6-3-504 Crimes against computer users; penalties.

(a) A person commits a crime against computer users if he knowingly and without authorization:

(i) Accesses a computer, computer system or computer network;

(ii) Denies computer system services to an authorized user of the computer system services which, in whole or part, are owned by, under contract to, or operated for, on behalf of, or in conjunction with another.

(b) A crime against computer users is:

(i) A felony punishable by imprisonment for not more than three (3) years, a fine of not more than three thousand dollars ($3,000.00), or both except as provided in paragraph (ii) of this subsection;

(ii) A felony punishable by imprisonment for not more than ten (10) years, a fine of not more than ten thousand dollars ($10,000.00), or both, if the crime is committed with the intention of devising or executing a scheme or artifice to defraud or to obtain property.

§6-3-505 This article not exclusive.

This article shall not preclude the application of any other provision of the criminal law of this state which applies, or may apply, to any violation of this article, unless the provision is inconsistent with this article.